FQ5-547 JP JPO ref 9

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平10－214233

(43)公開日　平成10年(1998) 8月11日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ
Ｇ０９Ｃ　1/00	６３０	Ｇ０９Ｃ　1/00	６３０Ａ
	６６０		６６０Ｄ
			６６０Ａ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ

審査請求　未請求　請求項の数25　ＯＬ　（全 29 頁）　最終頁に続く

(21)出願番号　特願平9－97583

(22)出願日　平成９年(1997) ４月15日

(31)優先権主張番号　特願平8－92516
(32)優先日　平８(1996) ４月15日
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平8－320291
(32)優先日　平８(1996)11月29日
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　清水　秀夫
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　遠藤　直樹
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　才所　敏明
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　弁理士　鈴江　武彦　（外６名）

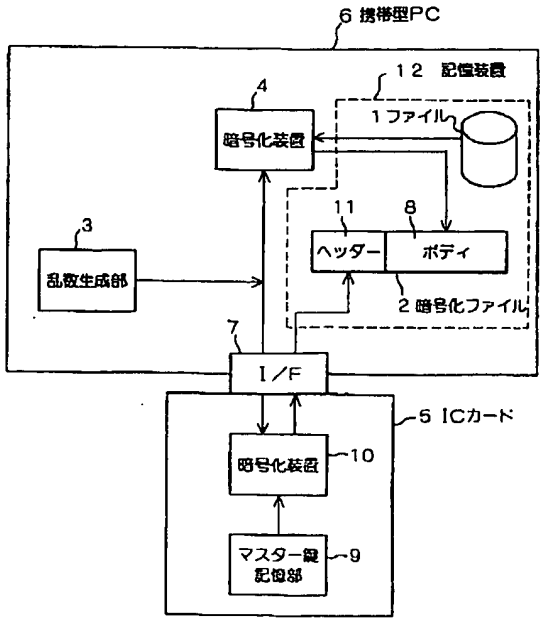
最終頁に続く

(54)【発明の名称】　**情報処理装置、情報処理システム、情報処理方法、プログラム記憶装置、及び鍵の判定方法及び判定装置**

(57)【要約】

【課題】たとえ装置が盗難されたり分解されたりしても、内部に記憶された機械情報を保護することができる情報処理システムを提供する。

【解決手段】携帯型ＰＣ６と、この携帯型ＰＣ６とは別体で構成されており、かつ携帯型ＰＣ６と信号の受渡しが可能なＩＣカード５とを具備する情報処理システムであって、携帯型ＰＣ６は、一時鍵を生成するための乱数生成部３と、一時鍵を用いてデータを暗号化してボディ部８を生成するための暗号化装置４とを備え、ＩＣカード５は、マスター鍵を記憶するためのマスター鍵記憶部９と、マスター鍵を用いて一時鍵を暗号化してヘッダー部１１を生成するための暗号化装置１０とを備え、携帯型ＰＣ６は、ボディ部８と、ヘッダー部１１とを合成して暗号化ファイル２として記憶するための記憶装置１２をさらに具備する。



【特許請求の範囲】

【請求項１】　第１の情報処理装置と、この第１の情報処理装置とは別体で構成されており、かつ前記第１の情報処理装置と信号の受渡しが可能な第２の情報処理装置とを具備する情報処理システムであって、

前記第１の情報処理装置は、

第１の鍵を生成するための第１鍵生成手段と、

この第１鍵生成手段によって生成された前記第１の鍵を用いてデータを暗号化して第１暗号情報を生成するための第１暗号化手段とを備え、

前記第２の情報処理装置は、

第２の鍵を記憶するための第２鍵記憶手段と、

この第２鍵記憶手段に記憶された前記第２の鍵を用いて前記第１の鍵を暗号化して第２暗号情報を生成するための第２暗号化手段と、を備え、

前記第１の情報処理装置は、前記第１暗号化手段によって生成された前記第１暗号情報と、前記第２暗号化手段によって生成された前記第２暗号情報とを関連付けて記憶するための関連付け記憶手段をさらに具備することを特徴とする情報処理システム。

【請求項２】　前記第１の暗号化手段は、前記第１暗号化情報を生成した後に、前記データを削除する手段を有する請求項１記載の情報処理システム。

【請求項３】　第１の情報処理装置と、この第１の情報処理装置とは別体で構成されており、かつ前記第１の情報処理装置と信号の受渡しが可能な第２の情報処理装置とを具備する情報処理システムであって、

前記第１の情報処理装置は、

第１の鍵によりデータを暗号化した第１暗号情報と、第２の鍵により第１の鍵を暗号化した第２暗号情報とを関連付けて記憶するための関連付け記憶手段を備え、

前記第２の情報処理装置は、

第２の鍵を記憶するための第２鍵記憶手段と、

この第２鍵記憶手段に記憶された前記第２の鍵により、前記関連付け記憶手段から読み出された前記第２暗号情報を復号して前記第１の鍵を取出すための第１復号手段と、を備え、

前記第１の情報処理装置は、前記第１復号手段によって取り出された前記第１の鍵により、前記関連付け記憶手段に記憶された前記第１暗号情報を復号して前記データを得るための第２復号手段をさらに具備することを特徴とする情報処理システム。

【請求項４】　第１の鍵を生成するための第１鍵生成手段と、

この第１鍵生成手段によって生成された前記第１の鍵によりデータを暗号化するための暗号化手段と、

前記第１鍵生成手段によって生成された前記第１の鍵を外部情報処理装置へ出力し、該外部情報処理装置内で当該装置内に記憶されている第２の鍵により暗号化された前記第１の鍵を入力するための入力手段と、

この入力手段を介して入力される前記暗号化された第１の鍵と、前記暗号化手段によって暗号化された前記データとを関連付けて記憶するための記憶手段と、を具備することを特徴とする情報処理装置。

【請求項５】　前記暗号化手段は、前記データを暗号化した後に、当該データを削除する手段を有することを特徴とする請求項４記載の情報処理装置。

【請求項６】　第１の鍵によりデータを暗号化した第１暗号情報と、第２の鍵により前記第１の鍵を暗号化した第２暗号情報とを記憶するための記憶手段と、

この記憶手段に記憶されている前記第２の暗号情報を外部情報処理装置へ出力し、該外部情報処理装置内で当該外部情報処理装置内に記憶されている第２の鍵により前記第２暗号情報を復号して得られる復号された第１の鍵を入力するための入力手段と、

この入力手段を介して入力された前記復号された第１の鍵により前記第１暗号情報を復号して前記データを得るための復号化手段とを具備することを特徴とする情報処理装置。

【請求項７】　第２の鍵を記憶するための記憶手段と、第１の鍵を生成し、この第１の鍵によりデータを暗号化する外部情報処理装置から、前記第１の鍵を入力するための入力手段と、

前記記憶手段に記憶されている前記第２の鍵によって、前記入力手段を介して入力される前記第１の鍵を暗号化するための暗号化手段と、

前記外部情報処理装置において、この暗号化手段によって暗号化された第１の鍵と、前記暗号化されたデータとを関連付けて記憶するために、前記暗号化された第１の鍵を前記外部情報処理装置へ出力するための出力手段と、を具備することを特徴とする情報処理装置。

【請求項８】　第２の鍵を記憶するための記憶手段と、第１の鍵によりデータを暗号化して得られる第１暗号情報と、前記記憶手段に記憶された前記第２の鍵により、前記第１の鍵を暗号化して得られる第２暗号情報とを記憶するための記憶手段を備えた外部情報処理装置から、前記第２暗号情報を入力するための入力手段と、

この入力手段を介して入力された前記第２暗号情報を前記第２の鍵により復号して前記第１の鍵を取出すための復号手段と、

前記外部情報処理装置において、前記復号手段により取り出された前記第１の鍵により前記第１暗号情報を復号して前記データを得るために、前記取り出された第１の鍵を前記外部情報処理装置へ出力するための出力手段と、を具備することを特徴とする情報処理装置。

【請求項９】　第１の情報処理装置内で第１の鍵を生成する第１鍵生成工程と、

生成された第１の鍵を用いてデータを暗号化して第１暗号情報を生成する第１暗号情報生成工程と、

生成された第１の鍵を、前記第１の情報処理装置とは別

体で構成され、第２の鍵を記憶している第２の情報処理装置へ出力する出力工程と、
前記第２の情報処理装置内で前記第２の鍵を用いて前記第１の鍵を暗号化して第２暗号情報を生成する第２暗号情報生成工程と、
生成された第２暗号情報を前記第１の情報処理装置へ出力する出力工程と、
前記第１情報処理装置内で前記第１暗号情報と前記第２暗号情報とを関連付けて記憶する記憶工程と、を具備することを特徴とする情報処理方法。

【請求項１０】　第１の鍵によりデータを暗号化して得られた第１暗号情報と、第２の鍵により前記第１の鍵を暗号化して得られた第２暗号情報とが関連付けて記憶されている第１の情報処理装置内から、前記第２暗号情報を、当該第１の情報処理装置とは別体で構成された第２の情報処理装置へ出力する出力工程と、
前記第２の情報処理装置内に予め記憶されている前記第２の鍵により、前記第２暗号情報を復号して前記第１の鍵を取り出す第１鍵取り出し工程と、
取り出された第１の鍵を前記第１の情報処理装置へ出力する出力工程と、
前記第１の情報処理装置において、当該第１の鍵により前記第１暗号情報を復号して前記データを得るデータ取得工程と、を具備することを特徴とする情報処理方法。

【請求項１１】　第１の鍵を生成する第１鍵生成工程と、
生成された第１の鍵によりデータを暗号化する暗号化工程と、
生成された第１の鍵を外部情報処理装置へ出力する出力工程と、
当該外部情報処理装置内で当該外部情報処理装置内に記憶されている第２の鍵により暗号化された第１の鍵を入力する入力工程と、
入力された前記暗号化された第１の鍵と、前記第１の鍵により暗号化されたデータとを関連付けて記憶する記憶工程と、を具備することを特徴とする情報処理方法。

【請求項１２】　第１の鍵によりデータを暗号化して記憶された第１暗号情報と、第２の鍵により第１の鍵を暗号化して記憶された第２暗号情報のうち、前記第２の暗号情報を外部情報処理装置へ出力する出力工程と、
該外部情報処理装置内で当該外部情報処理装置内に記憶されている前記第２の鍵により前記第２暗号情報を復号して得られた前記第１の鍵を入力する入力工程と、
入力された前記第１の鍵により前記第１暗号情報を復号して前記データを取り出す取り出し工程と、を具備することを特徴とする情報処理方法。

【請求項１３】　生成された第１の鍵によりデータを暗号化する外部情報処理装置から前記第１の鍵を入力する入力工程と、
予め記憶されている第２の鍵により入力された前記第１の鍵を暗号化する暗号化工程と、

前記外部情報処理装置において、この暗号化された第１の鍵と、前記暗号化されたデータとを関連付けて記憶するために、前記暗号化された第１の鍵を前記外部情報処理装置へ出力する出力工程と、を具備することを特徴とする情報処理方法。

【請求項１４】　第１の鍵によりデータを暗号化して得られた第１暗号情報と、第２の鍵により第１の鍵を暗号化して得られた第２暗号情報とを記憶するための記憶手段を備えた外部情報処理装置から前記第２暗号情報を入力する入力工程と、
予め記憶している第２の鍵により前記第２暗号情報を復号して前記第１の鍵を取出す取り出し工程と、
前記外部情報処理装置において、取り出された前記第１の鍵により前記第１暗号情報を復号して前記データを得るために、復号により取り出された前記第１の鍵を前記外部情報処理装置へ出力する出力工程と、を具備することを特徴とする情報処理方法。

【請求項１５】　暗号化処理を実行する方法ステップを遂行するために、マシーンによってリーダブルなプログラムを記憶したプログラム記憶装置であって、
前記方法ステップは、
第１の鍵を生成する第１鍵生成ステップと、
生成された第１の鍵によりデータを暗号化する暗号化ステップと、
生成された第１の鍵を外部情報処理装置へ出力する出力ステップと、
当該外部情報処理装置内で当該外部情報処理装置内に記憶されている第２の鍵により暗号化された第１の鍵を入力する入力ステップと、
入力された前記暗号化された第１の鍵と、前記第１の鍵により暗号化されたデータとを関連付けて記憶する記憶ステップと、を具備することを特徴とするプログラム記憶装置。

【請求項１６】　暗号化処理を実行する方法ステップを遂行するために、マシーンによってリーダブルなプログラムを記憶したプログラム記憶装置であって、
前記方法ステップは、
第１の鍵によりデータを暗号化して記憶された第１暗号情報と、第２の鍵により第１の鍵を暗号化して記憶された第２暗号情報のうち、前記第２の暗号情報を外部情報処理装置へ出力する出力ステップと、
該外部情報処理装置内で当該外部情報処理装置内に記憶されている前記第２の鍵により前記第２暗号情報を復号して得られた前記第１の鍵を入力する入力ステップと、
入力された前記第１の鍵により前記第１暗号情報を復号して前記データを取り出す取り出しステップと、を具備することを特徴とするプログラム記憶装置。

【請求項１７】　送信側で、データを暗号化するのに用いた第１の鍵を複数の第２の鍵でそれぞれ暗号化あるい

5

は復号して送信し、受信側で、前記複数の第２の鍵の中から受信側で有している特定の第２の鍵に該当する第２の鍵を前記複数の第２の鍵の中から抽出するための鍵の判定方法において、

前記第１の鍵を前記複数の第２の鍵でそれぞれ暗号化あるいは復号化して得られた第１データを入力する入力工程と、

前記第１データの中で前記特定の第２の鍵で暗号化あるいは復号化された特定の第１データと所定の処理を行なうことにより前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する入力工程と、

入力された前記第１データと前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出工程と、

抽出された前記特定の第２の鍵を出力する出力工程と、を具備することを特徴とする鍵の判定方法。

【請求項１８】　送信側で、データを暗号化するのに用いた第１の鍵を複数の第２の鍵の中の特定の第２の鍵で暗号化あるいは復号化して送信し、受信側で、前記複数の第２の鍵の中から前記特定の第２の鍵を抽出するための鍵の判定方法において、

前記第１の鍵を前記特定の第２の鍵で暗号化あるいは復号して得られた第１データを入力する入力工程と、

前記第１データと所定の処理を行なうことにより、前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する入力工程と、

入力された前記第１データと前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出工程と、

抽出された前記特定の第２の鍵を出力する出力工程と、を具備することを特徴とする鍵の判定方法。

【請求項１９】　送信側で、データを暗号化するのに用いた第１の鍵を送信側及び受信側が共に有している複数の第２の鍵の中から、特定の第２の鍵で暗号化あるいは復号して送信し、受信側で、前記特定の第２の鍵に該当する第２の鍵を前記複数の第２の鍵の中から抽出するための鍵の判定方法であって、

前記第１の鍵を前記特定の第２の鍵で暗号化あるいは復号して得られた第１データを入力する入力工程と、

前記第１データの中と所定の処理を行なうことにより前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する入力工程と、

入力された前記第１データと前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出工程と、

抽出された前記特定の第２の鍵を出力する出力工程と、を具備することを特徴とする鍵の判定方法。

【請求項２０】　送信側で、データを暗号化するのに用いた第１の鍵を複数の第２の鍵でそれぞれ暗号化あるいは復号して送信し、受信側で、前記複数の第２の鍵の中

6

から受信側で有している特定の第２の鍵に該当する第２の鍵を前記複数の第２の鍵の中から抽出するための鍵の判定装置であって、

前記第１の鍵を前記複数の第２の鍵でそれぞれ暗号化あるいは復号化して得られた第１データを入力する第１入力手段と、

この第１入力手段によって入力された前記第１データの中で、前記特定の第２の鍵で暗号化あるいは復号化された特定の第１データと所定の処理を行なうことにより前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する第２入力手段と、

この第１入力手段によって入力された前記第１データと、前記第２入力手段によって入力された前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出手段と、

この抽出手段によって抽出された前記特定の第２の鍵を出力する出力手段と、を具備することを特徴とする鍵の判定装置。

【請求項２１】　送信側で、データを暗号化するのに用いた第１の鍵を複数の第２の鍵の中の特定の第２の鍵で暗号化あるいは復号化して送信し、受信側で、前記複数の第２の鍵の中から前記特定の第２の鍵を抽出するための鍵の判定装置であって、

前記第１の鍵を前記特定の第２の鍵で暗号化あるいは復号して得られた第１データを入力する第１入力手段と、

この第１入力手段によって入力された前記第１データと所定の処理を行なうことにより、前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する第２入力手段と、

この第２入力手段によって入力された前記第１データと前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出手段と、

この抽出手段によって抽出された前記特定の第２の鍵を出力する出力手段と、を具備することを特徴とする鍵の判定装置。

【請求項２２】　送信側で、データを暗号化するのに用いた第１の鍵を送信側及び受信側が共に有している複数の第２の鍵の中から、特定の第２の鍵で暗号化あるいは復号して送信し、受信側で、前記特定の第２の鍵に該当する第２の鍵を前記複数の第２の鍵の中から抽出するための鍵の判定装置であって、

前記第１の鍵を前記特定の第２の鍵で暗号化あるいは復号して得られた第１データを入力する第１入力手段と、

この第１入力手段によって入力された前記第１データの中と所定の処理を行なうことにより前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する第２入力手段と、

前記第１入力手段によって入力された前記第１データと、前記第２入力手段によって入力された前記第２データとに基づいて、前記所定の処理を行なうことにより前

記特定の第２の鍵を抽出する抽出手段と、
この抽出手段によって抽出された前記特定の第２の鍵を出力する出力手段と、を具備することを特徴とする鍵の判定装置。

【請求項２３】　送信側で、データを暗号化するのに用いた第１の鍵を複数の第２の鍵でそれぞれ暗号化あるいは復号して送信し、受信側で、前記複数の第２の鍵の中から受信側で有している特定の第２の鍵に該当する第２の鍵を前記複数の第２の鍵の中から抽出して鍵の判定を行なう判定ステップを遂行するために、マシンリーダブルなプログラムを記憶したプログラム記憶装置であって、
前記判定ステップは、
前記第１の鍵を前記複数の第２の鍵でそれぞれ暗号化あるいは復号化して得られた第１データを入力する入力ステップと、
前記第１データの中で前記特定の第２の鍵で暗号化あるいは復号化された特定の第１データと所定の処理を行なうことにより前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する入力ステップと、
入力された前記第１データと前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出ステップと、
抽出された前記特定の第２の鍵を出力する出力ステップと、を具備することを特徴とするプログラム記憶装置。

【請求項２４】　受信側で、データを暗号化するのに用いた第１の鍵を複数の第２の鍵の中の特定の第２の鍵で暗号化あるいは復号化して送信し、受信側で、前記複数の第２の鍵の中から前記特定の第２の鍵を抽出して鍵の判定を行なう判定ステップを遂行するために、マシンリーダブルなプログラムを記憶したプログラム記憶装置であって、
前記判定ステップは、
前記第１の鍵を前記特定の第２の鍵で暗号化あるいは復号して得られた第１データを入力する入力ステップと、
前記第１データと所定の処理を行なうことにより、前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する入力ステップと、
入力された前記第１データと前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出ステップと、
抽出された前記特定の第２の鍵を出力する出力ステップと、を具備することを特徴とするプログラム記憶装置。

【請求項２５】　送信側で、データを暗号化するのに用いた第１の鍵を送信側及び受信側が共に有している複数の第２の鍵の中から、特定の第２の鍵で暗号化あるいは復号して送信し、受信側で、前記特定の第２の鍵に該当する第２の鍵を前記複数の第２の鍵の中から抽出して鍵の判定を行なう判定ステップを遂行するために、マシンリーダブルなプログラムを記憶したプログラム記憶装置であって、
前記判定ステップは、
前記第１の鍵を前記特定の第２の鍵で暗号化あるいは復号して得られた第１データを入力する入力ステップと、
前記第１データの中と所定の処理を行なうことにより前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する入力ステップと、
入力された前記第１データと前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出ステップと、
抽出された前記特定の第２の鍵を出力する出力ステップと、を具備することを特徴とするプログラム記憶装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は情報処理装置、情報処理システム、情報処理方法、記録媒体（プログラム記憶装置）、及び鍵の判定方法及び装置に関し、特に、ＩＣカード等との間で信号の受け渡しが可能な携帯型パーソナルコンピュータにおいて、ファイル暗号化システムを備えた情報処理装置、情報処理システム、情報処理方法、記録媒体、及び鍵の判定方法及び装置に関する。

【０００２】

【従来の技術】近年、技術の進歩によりコンピュータの小型化が進み、操作者が所望の場所に移動させて操作できる携帯型パーソナルコンピュータが登場している。このような携帯型パーソナルコンピュータはハードディスク等の大容量外部記憶装置を内蔵しており、携帯型であっても種々のアプリケーションプログラムや作成したファイルを記憶することが可能である。

【０００３】ところで、携帯型以外のコンピュータの場合は屋内に設置される場合が多いので、コンピュータが設置してある部屋への出入りを制限する等の方法によってコンピュータの内部に格納されている機密情報を不正な第３者から保護することが可能である。また、通信ネットワークの発展により、ローカルホストからリモートホストの内部に侵入して不正を行なうといったことが可能になったが、この場合でも、リモートホスト自体は物理的に隔絶された場所に配置されているのでリモートホスト自体に直接被害が及ぶということはない。

【０００４】ところが上記した携帯型パーソナルコンピュータにおいては、携帯が可能であるために、装置自体が盗難されてその内部に格納されている機密情報が盗まれてしまう可能性がある。そこで、パスワードなどを用いて、たとえ盗難されてもパスワードの保持者以外は使用できないようにする方法が考えられる。しかしながら、このような方法を用いたとしても装置自体を分解して内蔵されているハードディスクを取り出し、ハードディスクに格納されている機密情報を入手することが可能である。分解できないパーソナルコンピュータを製造す

ることは困難であり、仮に製造可能であったとしても、装置が大型になって携帯に適さなくなるとともに、製造コストが増大してしまうという問題が新たに発生する。

【０００５】また、近年、データを複数のユーザで共有するケースが増加してきている。例えば、１台のパーソナルコンピュータを複数のユーザで共用する形態においてそのパーソナルコンピュータに内蔵されたハードディスク装置内のデータを共有する場合、あるいは各ユーザのパーソナルコンピュータをＬＡＮなどで接続し、このＬＡＮに接続された記録装置を複数のユーザで共用する形態においてこの記録装置内のデータを共有する場合などである。

【０００６】従って、ユーザ個人のデータを安全に保存するだけでなく、複数のユーザで共有するデータで高い機密性を要するものについても安全性を確保する必要が生じている。

【０００７】しかし、同一データを複数のユーザ間で共有する場合、暗号鍵と復号鍵の対は、個人用に加えて、グループ用のものを用意し、同一データを、これを共有するユーザの個人用暗号鍵やグループ用暗号鍵夫々で暗号化して、同一の内容を持つ複数の暗号化データを作成し保存することになるため、鍵の種類が多くなるとともに、暗号化データの種類も多くなり、鍵情報と暗号化データの管理が困難になるという問題点があった。また、従来は、間違った鍵で暗号化データを復号したために、内容を破壊してしまうようなトラブルも生じる可能性があった。

【０００８】

【発明が解決しようとする課題】上記したように、携帯型パーソナルコンピュータの出現によって利便性が向上したが、携帯型であるがために装置自体が盗難されて内部に格納されている機密情報が不正な第三者に知られてしまうという問題がある。また、パスワード等により機密情報へのアクセスを制限した場合でも、装置自体を分解して内蔵されているハードディスクを取り出し、ハードディスクに格納されている機密情報を入手することが可能であるという問題がある。

【０００９】また、個人やグループが共有するデータを、各々のマスタ鍵により復号可能な形で暗号化し保存するためには、各々のマスタ鍵で暗号化したファイルを保存する必要があることから、ファイルのデータ量が多量になり、また暗号化に要する時間が長くなる問題点、マスタ鍵と暗号化データの管理が困難になる問題点、違うマスタ鍵での誤復号によりデータが破壊される可能性がある問題点など、種々の問題点があった。

【００１０】

【課題を解決するための手段】本発明の情報処理システムはこのような課題に着目してなされたものであり、その目的とするところは、たとえ装置が盗難されたり分解されたりしても、内部に記憶された機械情報を保護することができる情報処理装置、情報処理システム、情報処理方法、記録媒体、及び鍵の判定方法及び装置を提供することにある。

【００１１】また、本発明の他の目的は、複数のユーザで共有するデータを、効率的かつ安全に暗号化した形で保存できる情報処理装置、情報処理システム、情報処理方法、記録媒体、及び鍵の判定方法及び装置を提供することにある。

【００１２】上記の目的を達成するために、第１の発明に係る情報処理システムは、第１の情報処理装置と、この第１の情報処理装置とは別体で構成されており、かつ前記第１の情報処理装置と信号の受渡しが可能な第２の情報処理装置とを具備する情報処理システムであって、前記第１の情報処理装置は、第１の鍵を生成するための第１鍵生成手段と、この第１鍵生成手段によって生成された前記第１の鍵を用いてデータを暗号化して第１暗号情報を生成するための第１暗号化手段とを備え、前記第２の情報処理装置は、第２の鍵を記憶するための第２鍵記憶手段と、この第２鍵記憶手段に記憶された前記第２の鍵を用いて前記第１の鍵を暗号化して第２暗号情報を生成するための第２暗号化手段とを備え、前記第１の情報処理装置は、前記第１暗号化手段によって生成された前記第１暗号情報と、前記第２暗号化手段によって生成された前記第２暗号情報とを関連付けて記憶するための関連付け記憶手段をさらに具備する。

【００１３】また、第２の発明は、第１の発明において、前記第１の暗号化手段は、前記第１暗号化情報を生成した後に、前記データを削除する手段を有する。また、第３の発明は、第１の発明において、前記第２鍵記憶手段は複数の第２の鍵を記憶しており、前記第１の情報処理装置は、前記第２の情報処理装置に対して、前記複数の第２の鍵の中から、前記第１の鍵を暗号化するのに用いるべき第２の鍵を指示するための指示手段を有する。

【００１４】また、第４の発明に係る情報処理システムは、第１の情報処理装置と、この第１の情報処理装置とは別体で構成されており、かつ前記第１の情報処理装置と信号の受渡しが可能な第２の情報処理装置とを具備する情報処理システムであって、前記第１の情報処理装置は、第１の鍵によりデータを暗号化した第１暗号情報と、第２の鍵により第１の鍵を暗号化した第２暗号情報とを関連付けて記憶するための関連付け記憶手段を備え、前記第２の情報処理装置は、第２の鍵を記憶するための第２鍵記憶手段と、この第２鍵記憶手段に記憶された前記第２の鍵により、前記関連付け記憶手段から読み出された前記第２暗号情報を復号して前記第１の鍵を取出すための第１復号手段とを備え、前記第１の情報処理装置は、前記第１復号手段によって取り出された前記第１の鍵により、前記関連付け記憶手段に記憶された前記第１暗号情報を復号して前記データを得るための第２復

号手段をさらに具備する。

【００１５】また、第５の発明に係る情報処理装置は、第１の鍵を生成するための第１鍵生成手段と、この第１鍵生成手段によって生成された前記第１の鍵によりデータを暗号化するための暗号化手段と、前記第１鍵生成手段によって生成された前記第１の鍵を外部情報処理装置へ出力し、該外部情報処理装置内で当該装置内に記憶されている第２の鍵により暗号化された前記第１の鍵を入力するための入力手段と、この入力手段を介して入力される前記暗号化された第１の鍵と、前記暗号化手段によって暗号化された前記データとを関連付けて記憶するための記憶手段とを具備する。

【００１６】また、第６の発明は、第５の発明において、前記暗号化手段は、前記データを暗号化した後に、当該データを削除する手段を有する。また、第７の発明は、第５の発明において、前記外部情報処理装置に対して、複数の第２の鍵の中から、前記第１鍵を暗号化するのに用いるべき第２の鍵を指示する指示手段をさらに具備する。

【００１７】また、第８の発明に係る情報処理装置は、第１の鍵によりデータを暗号化した第１暗号情報と、第２の鍵により前記第１の鍵を暗号化した第２暗号情報とを記憶するための記憶手段と、この記憶手段に記憶されている前記第２の暗号情報を外部情報処理装置へ出力し、該外部情報処理装置内で当該外部情報処理装置内に記憶されている第２の鍵により前記第２暗号情報を復号して得られる復号された第１の鍵を入力するための入力手段と、この入力手段を介して入力された前記復号された第１の鍵により前記第１暗号情報を復号して前記データを得るための復号化手段とを具備する。

【００１８】また、第９の発明に係る情報処理装置は、第２の鍵を記憶するための記憶手段と、第１の鍵を生成し、この第１の鍵によりデータを暗号化する外部情報処理装置から、前記第１の鍵を入力するための入力手段と、前記記憶手段に記憶されている前記第２の鍵によって、前記入力手段を介して入力される前記第１の鍵を暗号化するための暗号化手段と、前記外部情報処理装置において、この暗号化手段によって暗号化された第１の鍵と、前記暗号化されたデータとを関連付けて記憶するために、前記暗号化された第１の鍵を前記外部情報処理装置へ出力するための出力手段とを具備する。

【００１９】また、第１０の発明は、第９の発明において、前記記憶手段は複数の第２の鍵を記憶しており、前記暗号化手段は、この複数の第２の鍵の中から、前記外部情報処理装置によって指示された第２の鍵によって前記第１の鍵を暗号化する手段を有する。

【００２０】また、第１１の発明に係る情報処理装置は、第２の鍵を記憶するための記憶手段と、第１の鍵によりデータを暗号化して得られる第１暗号情報と、前記記憶手段に記憶された前記第２の鍵により、前記第１の鍵を暗号化して得られる第２暗号情報とを記憶するための記憶手段を備えた外部情報処理装置から、前記第２暗号情報を入力するための入力手段と、この入力手段を介して入力された前記第２暗号情報を前記第２の鍵により復号して前記第１の鍵を取出すための復号手段と、前記外部情報処理装置において、前記復号手段により取り出された前記第１の鍵により前記第１暗号情報を復号して前記データを得るために、前記取り出された第１の鍵を前記外部情報処理装置へ出力するための出力手段とを具備する。

【００２１】また、第１２の発明に係る情報処理方法は、第１の情報処理装置内で第１の鍵を生成する第１鍵生成工程と、生成された第１の鍵を用いてデータを暗号化して第１暗号情報を生成する第１暗号情報生成工程と、生成された第１の鍵を、前記第１の情報処理装置とは別体で構成され、第２の鍵を記憶している第２の情報処理装置へ出力する出力工程と、前記第２の情報処理装置内で前記第２の鍵を用いて前記第１の鍵を暗号化して第２暗号情報を生成する第２暗号情報生成工程と、生成された第２暗号情報を前記第１の情報処理装置へ出力する出力工程と、前記第１情報処理装置内で前記第１暗号情報と前記第２暗号情報とを関連付けて記憶する記憶工程とを具備する。

【００２２】また、第１３の発明に係る情報処理方法は、第１の鍵によりデータを暗号化して得られた第１暗号情報と、第２の鍵により前記第１の鍵を暗号化して得られた第２暗号情報とが関連付けて記憶されている第１の情報処理装置内から、前記第２暗号情報を、当該第１の情報処理装置とは別体で構成された第２の情報処理装置へ出力する出力工程と、前記第２の情報処理装置内に予め記憶されている前記第２の鍵により、前記第２暗号情報を復号して前記第１の鍵を取り出す第１鍵取り出し工程と、取り出された第１の鍵を前記第１の情報処理装置へ出力する出力工程と、前記第１の情報処理装置において、当該第１の鍵により前記第１暗号情報を復号して前記データを得るデータ取得工程とを具備する。

【００２３】また、第１４の発明に係る情報処理方法は、第１の鍵を生成する第１鍵生成工程と、生成された第１の鍵によりデータを暗号化する暗号化工程と、生成された第１の鍵を外部情報処理装置へ出力する出力工程と、当該外部情報処理装置内で当該外部情報処理装置内に記憶されている第２の鍵により暗号化された第１の鍵を入力する入力工程と、入力された前記暗号化された第１の鍵と、前記第１の鍵により暗号化されたデータとを関連付けて記憶する記憶工程とを具備する。

【００２４】また、第１５の発明に係る情報処理方法は、第１の鍵によりデータを暗号化して記憶された第１暗号情報と、第２の鍵により第１の鍵を暗号化して記憶された第２暗号情報のうち、前記第２の暗号情報を外部情報処理装置へ出力する出力工程と、該外部情報処理装

置内で当該外部情報処理装置内に記憶されている前記第２の鍵により前記第２暗号情報を復号して得られた前記第１の鍵を入力する入力工程と、入力された前記第１の鍵により前記第１暗号情報を復号して前記データを取り出す取り出し工程とを具備する。

【００２５】また、第１６の発明に係る情報処理方法は、生成された第１の鍵によりデータを暗号化する外部情報処理装置から前記第１の鍵を入力する入力工程と、予め記憶されている第２の鍵により入力された前記第１の鍵を暗号化する暗号化工程と、前記外部情報処理装置において、この暗号化された第１の鍵と、前記暗号化されたデータとを関連付けて記憶するために、前記暗号化された第１の鍵を前記外部情報処理装置へ出力する出力工程とを具備する。

【００２６】また、第１７の発明に係る情報処理方法は、第１の鍵によりデータを暗号化して得られた第１暗号情報と、第２の鍵により第１の鍵を暗号化して得られた第２暗号情報とを記憶するための記憶手段を備えた外部情報処理装置から前記第２暗号情報を入力する入力工程と、予め記憶している第２の鍵により前記第２暗号情報を復号して前記第１の鍵を取出す取り出し工程と、前記外部情報処理装置において、取り出された前記第１の鍵により前記第１暗号情報を復号して前記データを得るために、復号により取り出された前記第１の鍵を前記外部情報処理装置へ出力する出力工程とを具備する。

【００２７】また、第１８の発明にプログラム記憶装置は、暗号化処理を実行する方法ステップを遂行するために、マシーンによってリーダブルなプログラムを記憶したプログラム記憶装置であって、前記方法ステップは、第１の鍵を生成する第１鍵生成ステップと、生成された第１の鍵によりデータを暗号化する暗号化ステップと、生成された第１の鍵を外部情報処理装置へ出力する出力ステップと、当該外部情報処理装置内で当該外部情報処理装置内に記憶されている第２の鍵により暗号化された第１の鍵を入力する入力ステップと、入力された前記暗号化された第１の鍵と、前記第１の鍵により暗号化されたデータとを関連付けて記憶する記憶ステップとを具備する。

【００２８】また、第１９の発明に係るプログラム記憶装置は、暗号化処理を実行する方法ステップを遂行するために、マシーンによってリーダブルなプログラムを記憶したプログラム記憶装置であって、前記方法ステップは、第１の鍵によりデータを暗号化して記憶された第１暗号情報と、第２の鍵により第１の鍵を暗号化して記憶された第２暗号情報のうち、前記第２の暗号情報を外部情報処理装置へ出力する出力ステップと、該外部情報処理装置内で当該外部情報処理装置内に記憶されている前記第２の鍵により前記第２暗号情報を復号して得られた前記第１の鍵を入力する入力ステップと、入力された前記第１の鍵により前記第１暗号情報を復号して前記データを取り出す取り出しステップとを具備する。

【００２９】また、第２０の発明に係る鍵の判定方法は、送信側で、データを暗号化するのに用いた第１の鍵を複数の第２の鍵でそれぞれ暗号化あるいは復号して送信し、受信側で、前記複数の第２の鍵の中から受信側で有している特定の第２の鍵に該当する第２の鍵を前記複数の第２の鍵の中から抽出するための鍵の判定方法において、前記第１の鍵を前記複数の第２の鍵でそれぞれ暗号化あるいは復号化して得られた第１データを入力する入力工程と、前記第１データの中で前記特定の第２の鍵で暗号化あるいは復号化された特定の第１データと所定の処理を行なうことにより前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する入力工程と、入力された前記第１データと前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出工程と、抽出された前記特定の第２の鍵を出力する出力工程とを具備する。

【００３０】また、第２１の発明に係る鍵の判定方法は、送信側で、データを暗号化するのに用いた第１の鍵を複数の第２の鍵の中の特定の第２の鍵で暗号化あるいは復号化して送信し、受信側で、前記複数の第２の鍵の中から前記特定の第２の鍵を抽出するための鍵の判定方法において、前記第１の鍵を前記特定の第２の鍵で暗号化あるいは復号して得られた第１データを入力する入力工程と、前記第１データと所定の処理を行なうことにより、前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する入力工程と、入力された前記第１データと前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出工程と、抽出された前記特定の第２の鍵を出力する出力工程とを具備する。

【００３１】また、第２２の発明に係る鍵の判定方法は、送信側で、データを暗号化するのに用いた第１の鍵を送信側及び受信側が共に有している複数の第２の鍵の中から、特定の第２の鍵で暗号化あるいは復号して送信し、受信側で、前記特定の第２の鍵に該当する第２の鍵を前記複数の第２の鍵の中から抽出するための鍵の判定方法であって、前記第１の鍵を前記特定の第２の鍵で暗号化あるいは復号して得られた第１データを入力する入力工程と、前記第１データの中と所定の処理を行なうことにより前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する入力工程と、入力された前記第１データと前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出工程と、抽出された前記特定の第２の鍵を出力する出力工程とを具備する。

【００３２】また、第２３の発明に係る鍵の判定装置は、送信側で、データを暗号化するのに用いた第１の鍵を複数の第２の鍵でそれぞれ暗号化あるいは復号して送信し、受信側で、前記複数の第２の鍵の中から受信側で

有している特定の第２の鍵に該当する第２の鍵を前記複数の第２の鍵の中から抽出するための鍵の判定装置であって、前記第１の鍵を前記複数の第２の鍵でそれぞれ暗号化あるいは復号化して得られた第１データを入力する第１入力手段と、この第１入力手段によって入力された前記第１データの中で、前記特定の第２の鍵で暗号化あるいは復号化された特定の第１データと所定の処理を行なうことにより前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する第２入力手段と、この第１入力手段によって入力された前記第１データと、前記第２入力手段によって入力された前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出手段と、この抽出手段によって抽出された前記特定の第２の鍵を出力する出力手段とを具備する。

【００３３】また、第２４の発明は、第２３の発明において、前記第２のデータを前記第１の鍵と前記第２の鍵とに基づいて生成する第１生成手段と、前記第２のデータを前記第１の鍵のみに基づいて生成する第２生成手段と、前記第２データを前記第２の鍵のみに基づいて生成する第３生成手段と、前記第２データを前記第１の鍵と前記第２の鍵のいずれをも使用しないで生成する第４の生成手段をさらに具備する。

【００３４】また、第２５の発明は、第２４の発明において、前記第１生成手段は、前記第２の鍵を前記第１の鍵で暗号化して得られるデータと、前記第２の鍵を前記第１の鍵で復号して得られるデータと、前記第１の鍵を前記第２の鍵で２回暗号化して得られるデータと、前記第１の鍵を前記第２の鍵で復号して得られるデータのいずれかを選択的に生成する。

【００３５】また、第２６の発明は、第２４の発明において、前記第２生成手段は、前記第１の鍵をこの第１の鍵で暗号化して得られるデータと、前記第１の鍵をこの第１の鍵で復号して得られるデータと、所定の共有データを前記第１の鍵で暗号化して得られるデータと、所定の共有データを前記第１の鍵で復号して得られるデータと、前記第１の鍵を特定の関数で暗号化して得られるデータのいずれかを選択的に生成する。

【００３６】また、第２７の発明は、第２４の発明において、前記第３生成手段は、前記第２の鍵をこの第２の鍵で暗号化して得られるデータと、前記第２の鍵を前記第２の鍵で復号して得られるデータと、前記第２の鍵と暗号化ごとに変更される共有データとを加算したものを前記第２の鍵で暗号化して得られるデータと、前記第２の鍵と暗号化ごとに変更される共有データとを加算したものを前記第２の鍵で復号して得られるデータと、暗号化ごとに変更される共有データを前記第２の鍵で暗号化して得られるデータと、暗号化ごとに変更される共有データを前記第２の鍵で復号して得られるデータと、前記第２の鍵を特定の関数で暗号化して得られるデータのいずれかを選択的に生成する。

【００３７】また、第２８の発明は、第２４の発明において、前記第４生成手段は、前記第１の鍵と前記第２の鍵とを並置したデータを特定の関数で暗号化して得られるデータを生成する。

【００３８】また、第２９の発明に係る鍵の判定装置は、送信側で、データを暗号化するのに用いた第１の鍵を複数の第２の鍵の中の特定の第２の鍵で暗号化あるいは復号化して送信し、受信側で、前記複数の第２の鍵の中から前記特定の第２の鍵を抽出するための鍵の判定装置であって、前記第１の鍵を前記特定の第２の鍵で暗号化あるいは復号して得られた第１データを入力する第１入力手段と、この第１入力手段によって入力された前記第１データと所定の処理を行なうことにより、前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する第２入力手段と、この第２入力手段によって入力された前記第１データと前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出手段と、この抽出手段によって抽出された前記特定の第２の鍵を出力する出力手段とを具備する。

【００３９】また、第３０の発明は、第２９の発明において、前記第２データを前記第１の鍵と前記第２の鍵とに基づいて生成する第１生成手段と、前記第２のデータを前記第１の鍵のみに基づいて生成する第２生成手段と、前記第２データを前記第２の鍵のみに基づいて生成する第３生成手段と、前記第２データを前記第１の鍵と前記第２の鍵のいずれをも使用しないで生成する第４の生成手段をさらに具備する。

【００４０】また、第３１の発明は、第３０の発明において、前記第１生成手段は、前記第２の鍵を前記第１の鍵で暗号化した得られるデータと、前記第２の鍵を前記第１の鍵で復号して得られるデータと、前記第１の鍵を前記第２の鍵で２回暗号化して得られるデータと、前記第１の鍵を前記第２の鍵で復号して得られるデータのいずれかを選択的に生成する。

【００４１】また、第３２の発明は、第３０の発明において、前記第２生成手段は、前記第１の鍵をこの第１の鍵で暗号化して得られるデータと、前記第１の鍵をこの第１の鍵で復号して得られるデータと、所定の共有データを前記第１の鍵で暗号化して得られるデータと、所定の共有データを前記第１の鍵で復号して得られるデータと、前記第１の鍵を特定の関数で暗号化して得られるデータのいずれかを選択的に生成する。

【００４２】また、第３３の発明は、第３０の発明において、前記第３判定手段は、前記第２の鍵をこの第２の鍵で暗号化して得られるデータと、前記第２の鍵を前記第２の鍵で復号して得られるデータと、前記第２の鍵と暗号化ごとに変更される共有データとを加算したものを前記第２の鍵で暗号化して得られるデータと、前記第２

の鍵と暗号化ごとに変更される共有データとを加算したものを前記第２の鍵で復号して得られるデータと、暗号化ごとに変更される共有データを前記第２の鍵で暗号化して得られるデータと、暗号化ごとに変更される共有データを前記第２の鍵で復号して得られるデータと、前記第２の鍵を特定の関数で暗号化して得られるデータのいずれかを選択的に生成する。

【００４３】また、第３４の発明は、第３０の発明において、前記第４生成手段は、前記第１の鍵と前記第２の鍵とを並置したデータを特定の関数で暗号化して得られるデータを生成する。

【００４４】また、第３５の発明に係る鍵の判定装置は、送信側で、データを暗号化するのに用いた第１の鍵を送信側及び受信側が共に有している複数の第２の鍵の中から、特定の第２の鍵で暗号化あるいは復号して送信し、受信側で、前記特定の第２の鍵に該当する第２の鍵を前記複数の第２の鍵の中から抽出するための鍵の判定装置であって、前記第１の鍵を前記特定の第２の鍵で暗号化あるいは復号して得られた第１データを入力する第１入力手段と、この第１入力手段によって入力された前記第１データの中と所定の処理を行なうことにより前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する第２入力手段と、前記第１入力手段によって入力された前記第１データと、前記第２入力手段によって入力された前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出手段と、この抽出手段によって抽出された前記特定の第２の鍵を出力する出力手段とを具備する。

【００４５】また、第３６の発明は、第３５の発明において、前記第２データを前記第１の鍵と前記第２の鍵とに基づいて生成する第１生成手段と、前記第２のデータを前記第１の鍵のみに基づいて生成する第２生成手段と、前記第２データを前記第２の鍵のみに基づいて生成する第３生成手段と、前記第２データを前記第１の鍵と前記第２の鍵のいずれをも使用しないで生成する第４の生成手段をさらに具備する。

【００４６】また、第３７の発明は、第３６の発明において、前記第１生成手段は、前記第２の鍵を前記第１の鍵で暗号化した得られるデータと、前記第２の鍵を前記第１の鍵で復号して得られるデータと、前記第１の鍵を前記第２の鍵で２回暗号化して得られるデータと、前記第１の鍵を前記第２の鍵で復号して得られるデータのいずれかを選択的に生成する。

【００４７】また、第３８の発明は、第３６の発明において、前記第２生成手段は、前記第１の鍵をこの第１の鍵で暗号化して得られるデータと、前記第１の鍵をこの第１の鍵で復号して得られるデータと、所定の共有データを前記第１の鍵で暗号化して得られるデータと、所定の共有データを前記第１の鍵で復号して得られるデータと、前記第１の鍵を特定の関数で暗号化して得られるデータのいずれかを選択的に生成する。

【００４８】また、第３９の発明は、第３６の発明において、前記第３生成手段は、前記第２の鍵をこの第２の鍵で暗号化して得られるデータと、前記第２の鍵を前記第２の鍵で復号して得られるデータと、前記第２の鍵と暗号化ごとに変更される共有データとを加算したものを前記第２の鍵で暗号化して得られるデータと、前記第２の鍵と暗号化ごとに変更される共有データとを加算したものを前記第２の鍵で復号して得られるデータと、暗号化ごとに変更される共有データを前記第２の鍵で暗号化して得られるデータと、暗号化ごとに変更される共有データを前記第２の鍵で復号して得られるデータと、前記第２の鍵を特定の関数で暗号化して得られるデータのいずれかを選択的に生成する。

【００４９】また、第４０の発明は、第３６の発明において、前記第４生成手段は、前記第１の鍵と前記第２の鍵とを並置したデータを特定の関数で暗号化して得られるデータを生成する。

【００５０】また、第４１の発明に係るプログラム記憶装置は、送信側で、データを暗号化するのに用いた第１の鍵を複数の第２の鍵でそれぞれ暗号化あるいは復号して送信し、受信側で、前記複数の第２の鍵の中から受信側で有している特定の第２の鍵に該当する第２の鍵を前記複数の第２の鍵の中から抽出して鍵の判定を行なう判定ステップを遂行するために、マシンリーダブルなプログラムを記憶したプログラム記憶装置であって、前記判定ステップは、前記第１の鍵を前記複数の第２の鍵でそれぞれ暗号化あるいは復号化して得られた第１データを入力する入力ステップと、前記第１データの中で前記特定の第２の鍵で暗号化あるいは復号化された特定の第１データと所定の処理を行なうことにより前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する入力ステップと、入力された前記第１データと前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出ステップと、抽出された前記特定の第２の鍵を出力する出力ステップとを具備する。

【００５１】また、第４２の発明に係るプログラム記憶装置は、送信側で、データを暗号化するのに用いた第１の鍵を複数の第２の鍵の中の特定の第２の鍵で暗号化あるいは復号化して送信し、受信側で、前記複数の第２の鍵の中から前記特定の第２の鍵を抽出して鍵の判定を行なう判定ステップを遂行するために、マシンリーダブルなプログラムを記憶したプログラム記憶装置であって、前記判定ステップは、前記第１の鍵を前記特定の第２の鍵で暗号化あるいは復号して得られた第１データを入力する入力ステップと、前記第１データと所定の処理を行なうことにより、前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する入力ステ

ップと、入力された前記第１データと前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出ステップと、抽出された前記特定の第２の鍵を出力する出力ステップとを具備する。

【００５２】また、第４３の発明に係るプログラム記憶装置は、送信側で、データを暗号化するのに用いた第１の鍵を送信側及び受信側が共に有している複数の第２の鍵の中から、特定の第２の鍵で暗号化あるいは復号して送信し、受信側で、前記特定の第２の鍵に該当する第２の鍵を前記複数の第２の鍵の中から抽出して鍵の判定を行なう判定ステップを遂行するために、マシンリーダブルなプログラムを記憶したプログラム記憶装置であって、前記判定ステップは、前記第１の鍵を前記特定の第２の鍵で暗号化あるいは復号して得られた第１データを入力する入力ステップと、前記第１データの中と所定の処理を行なうことにより前記特定の第２の鍵が得られるような処理によって処理された第２データを入力する入力ステップと、入力された前記第１データと前記第２データとに基づいて、前記所定の処理を行なうことにより前記特定の第２の鍵を抽出する抽出ステップと、抽出された前記特定の第２の鍵を出力する出力ステップとを具備する。

【００５３】

【発明の実施の形態】以下、図面を参照して、本発明の実施形態を詳細に説明する。図１は、本発明の第１の実施の形態に係る情報処理システムが適用される携帯型情報処理システムにおいて、暗号化を行なう場合の装置構成を示す図である。

【００５４】本発明の情報処理システムは、情報処理装置としての携帯型パーソナルコンピュータ（以下携帯型ＰＣと呼ぶ）６と、この携帯型ＰＣ６に着脱可能に装着された外部記憶装置としてのＩＣカード５とからなる。

【００５５】図１において、携帯型ＰＣ６内部に設けられた第１鍵生成手段としての乱数生成器３によって生成された一時鍵（第１の鍵）は暗号化装置４（第１暗号化手段）に転送される。また、携帯型ＰＣ６内部の例えばハードディスク装置等から成る記憶装置１２内に一時的に記憶されている機密情報を含むファイル１も、暗号化装置４に転送される。

【００５６】この暗号化装置４において機密情報を含むファイル１に対する暗号化が行われて暗号化ファイル２の第１の暗号化データとしてのボディ部８となる。一方、乱数発生器３によって生成された一時鍵は同時に外部インターフェース（以下外部Ｉ／Ｆと呼ぶ）７を介してＩＣカード５内部の第２の暗号化手段としての暗号化装置１０にも転送される。暗号化装置１０はマスター鍵記憶部（第２鍵記憶手段）９に記憶されているマスター鍵（第２の鍵）を用いて、転送された一時鍵を暗号化し、暗号化された一時鍵は外部Ｉ／Ｆ７を介して携帯型ＰＣ６内部の記憶装置（関連付け記憶手段）１２に転送されて暗号化ファイル２の第２の暗号化データとしてのヘッダー部１１となる。

【００５７】また、ＩＣカード５内に乱数発生器３を設けて、ＩＣカード３の内部で一時鍵を生成することも可能である。このようにすれば携帯型ＰＣ６とのデータ転送回数を減らすことができる。

【００５８】このようにしてファイル１に対する暗号化が行われ、ヘッダー１１とボディ部８とを合成することにより得られた暗号化ファイル２は記憶装置１２に記憶されると同時に、元のファイル１を消去する。

【００５９】図２は、暗号化を行った後の携帯型情報処理システムの構成の変更を示す図である。つまり、ファイル１を暗号化して暗号化ファイル２として記憶装置１２に記憶する一方で、元の機密情報を含むファイル１は記憶装置１２内からは削除される。またマスター鍵を記憶しているＩＣカード５を携帯型ＰＣ６から取り外し、携帯型ＰＣ６とＩＣカード５とを別々に保管する。

【００６０】すなわち、暗号化ファイル２として記憶されるのは、元のファイル１を暗号化した情報（ボディ部８）と暗号化の時に使用した一時鍵をマスター鍵で暗号化した情報（ヘッダー部１１）であり、いずれも暗号化された情報である。この暗号ファイル２のみを記憶した携帯型ＰＣ６が仮に盗難にあったとしても、マスター鍵を記憶したＩＣカード５を携帯型ＰＣ６と別に保管しておくことにより、マスター鍵と暗号化情報が同時に盗難にあうことを防止でき、機密情報の漏洩は防止される。

【００６１】なお、携帯型ＰＣ６内部の暗号化装置４で使用されるアルゴリズムと、ＩＣカード５内部の暗号化装置１０で使用されるアルゴリズムは同一のものであってもよいし、異なるアルゴリズムであってもよい。

【００６２】また、暗号化のための一時鍵は乱数発生装置により発生されたものなので例えば、ファイル毎に異なるものであり、より安全性が高まっている。図３は本発明の第１の実施の形態に係る情報処理システムが適用される携帯型情報処理システムにおいて、復号化を行なう場合の装置構成を示す図である。

【００６３】この図３は、基本的に図１に示したシステム構成図に対して、暗号化の機能と復号化の機能を入れ替えた構成に対応し、実際の情報処理システムでは、これら暗号化の機能と復号化の機能の双方を備えたものが用いられる。ここでは、図１の暗号化の機能と図３に示す復号化の機能が同一の携帯型情報処理システム内で処理されることを想定し、同一構成、同一要素には同一記号を付して説明する。

【００６４】図３における情報処理システムは、情報処理装置としての携帯型ＰＣ６と、この携帯型ＰＣ６に着脱可能に装着された外部記憶装置としてのＩＣカード５とからなる。

【００６５】図３において、携帯型ＰＣ６内部の暗号化

ファイル２はヘッダー部１１とボディ部８とに分解され、ヘッダー部１１は外部Ｉ／Ｆ７を介してＩＣカード５内部の第１の復号手段としての復号装置２０に転送される。復号装置２０はマスター鍵記憶部９に記憶されているマスター鍵を用いて復号を行って暗号化時に使用された元の一時鍵を抽出し、抽出された一時鍵を外部Ｉ／Ｆ７を介して携帯型ＰＣ６内部の第２復号手段としての復号装置１４に転送する。復号装置１４はこの一時鍵を用いて分解されたボディ部８の復号を行って元のファイル１を得る。

【００６６】以上、上記した第１の実施の形態によれば、暗号化ファイルは、携帯型ＰＣに対して着脱可能に装着されたＩＣカードに格納されたマスター鍵により暗号化した上で内部のハードディスクに保存されているので、ＩＣカードを装着しない限りファイルの復号はできない。したがってＩＣカードをＰＣとは別に携帯するようにすれば、たとえ携帯型ＰＣが盗難されても機密情報は安全に保護される。

【００６７】また、ファイル自体の暗号化は一時鍵を用いて携帯型ＰＣの内部を行い、外部から装着されるＩＣカードでは一時鍵のみをマスター鍵によって暗号化しているので、暗号化の効率が向上するとともに、携帯型ＰＣの内部にはマスター鍵が読み込まれることがなく、かつ２重に暗号化を行っていることになるので、機密情報の安全性がより向上する。

【００６８】また、計算能力のあるＩＣカード内にマスター鍵を格納した場合でも、マスター鍵自体は携帯型ＰＣ内に読み込まれて記憶されることはないので、例えば、トロイの木馬などのようなプログラムが携帯型ＰＣ内に組み込まれてもマスター鍵を不正な第三者に知られることはない。

【００６９】また、計算能力の異なるＩＣカードを適宜選択的に用いるようにすれば、暗号化、復号化時の処理を高速化することが可能である。これより、処理速度を重視しない場合は処理能力の劣るＩＣカードを用いてもよい。

【００７０】また、ファイル毎に鍵を変更しているので安全性がより高い。さらに、仮にマスター鍵が知られてしまってファイルを再び暗号化しなおさなければならない場合であっても、ヘッダー部のみを暗号化しなおすだけでよいので、短時間に暗号化を行うことができるという効果を奏する。

【００７１】また、ＤＥＳ暗号においては、十分な数のファイルと暗号化ファイルとの対を収集することによって暗号化に用いられた鍵を導き出されることが知られているが、上記した実施形態によれば、ファイルを暗号化するたび鍵に変更している上に、マスター鍵による暗号化部分に対応する平文ファイルが復号時に携帯型ＰＣ内に格納されることはないので、ファイルの収集そのものが不可能であり、仮にファイルの収集ができたとしても、十分な数のファイルが収集されるまで暗号化処理を繰り返すことは実質的に不可能である。すなわち、マスター鍵によりファイルを直接暗号化する方法では、たとえ数回の暗号化であっても、暗号化するファイルが十分に長ければ暗号化に用いられた鍵を導き出すことができる場合があるが、本実施形態ではマスター鍵自体はファイルを直接暗号化するためには用いられないので、十分に長いファイルを暗号化しても、鍵を導き出すのに十分なファイルを収集することはできない。

【００７２】なお、上記した実施形態ではマスター鍵で暗号化した一時鍵を記憶するヘッダー部が１つの場合について説明したが、ヘッダー部は複数であってもよい。例えば、１台のＰＣを複数人で構成されるグループ内で使用して情報を共有したい場合は、各人が個々に使用する暗号化鍵と、そのグループ内で共通に使用できる暗号化鍵とが必要になるので、ヘッダー部は複数用意することになる。また、あらかじめ複数のヘッダー部を設けて複数の人が内部のファイルにアクセスできるようにしておくことにより、何らかの理由でアクセスできなくなった人の代わりに他の人がアクセスして情報を得ることができる。

【００７３】また、上記した実施形態では携帯型ＰＣに着脱可能なＩＣカードを用いて情報処理装置と外部記憶装置との間で信号の受け渡しを行っているが、機械的に着脱可能に構成されていなくとも、例えば赤外線、無線、光（レーザ光等）通信などの方法により、情報処理装置と外部記憶装置との間で信号を受け渡すように構成してもよい。

【００７４】図４は、本発明の第２実施形態として、図１乃至図３に示した情報処理システムに適用することが可能な、鍵の判定方法を実現するための鍵判定システムの構成図である。特に、図４は復号時に用いられるマスター鍵を判定しながら、一時鍵を取り出す場合の装置構成を示す図である。ここでは暗号化時に、例えば図１のマスター鍵記憶部９に記憶されたマスター鍵を用いて暗号化された一時鍵をさらにマスター鍵で暗号化して得られた一時鍵（マスター鍵によって２回暗号化した一時鍵：第３の暗号化データ）が暗号化ファイルのヘッダー部１１にあらかじめ記憶されているものとする。

【００７５】そして、復号時には、図４に示すように第３の暗号化データとしての２回暗号化した一時鍵２３と、第２の暗号化データとしての１回暗号化した一時鍵２４とがＩＣカード５に供給される。復号装置２０ａは、マスター鍵記憶部９に記憶されたマスター鍵（特定のマスター鍵）を用いて２回暗号化した一時鍵２３を復号して復号された一時鍵を出力する。比較部２７はこの復号された一時鍵と、一回暗号化した一時鍵２４とを比較して比較結果を一致判定部３３に供給する。一致判定部３３はこの比較結果に基づいて、復号された一時鍵と１回暗号化した一時鍵とが一致するか否かを判定する。

【００７６】そして、一致すると判定された場合は一致信号２８によってスイッチ３４を閉じ、復号装置２０ａからの復号された一時鍵を復号装置２０ｂにおいてマスター鍵記憶部９に記憶されたマスター鍵を用いてさらに復号して元の一時鍵３１を得る。なお、図３のシステムに適用される場合には、ここで得られた元の一時鍵３１は、携帯型ＰＣ６へ転送されて暗号ファイル２の復号に使用される。なお、復号装置２０ａと２０ｂとは、機能ブロック上、２つの復号装置として示したが、実際には１つの復号化装置で良い。

【００７７】また、一致判定部３３で復号された一時鍵と１回暗号化した一時鍵２４が一致しないと判定された場合は、不一致信号２９が出力されてＮＧの状態３２が得られる。

【００７８】以上、上記した第２の実施の形態によれば、２回暗号化した一時鍵をマスター鍵によって復号した一時鍵と、１回暗号化した一時鍵とを比較することによって一致した場合は、復号に使用したマスター鍵が暗号化時に用いられたマスター鍵と同じ鍵であると判定することができ、一致しない場合は暗号化時に使用されたマスター鍵とは異なるマスター鍵によって一時鍵が復号されたと判定することができる。

【００７９】したがって、一致しない場合は当該マスター鍵を使用不可にすることにより、機密ファイルの漏洩を防止することができるとともに、誤ってファイルを破壊してしまうことを防止することができる。さらに、一台の携帯型ＰＣを複数人で使用する場合において、他人が暗号化したファイルを誤って復号してしまったときは一時鍵が失われてしまうので、もう一度暗号化しても元のファイルを復元することができないが、上記したように１回暗号化した一時鍵と、２回暗号化した一時鍵を復号した鍵とが一致しない場合は復号が行われないので、誤った一時鍵による復号を防止することができる。

【００８０】なお、上記した図４の装置を構成を簡略化すると図５に示すような構成となる。図５において、S_k は一時鍵、M_k はマスター鍵を表し、一時鍵S_k をマスター鍵M_k によって１回暗号化して得られるデータ（図４の２４）をM_k （S_k ）で表す。また、Ｄは復号を表している。M_k^2 （S_k ）はマスター鍵によって２回暗号化して得られるデータ（図４の２３）を表している。５１、５２は復号装置であり、図４の復号装置２０ａ、２０ｂにそれぞれ対応する。また、５３は比較判定部であり、図４の比較部２７、一致判定部３３に対応する。

【００８１】図６は図５に示す装置構成の変形例を示す図であり、２つの復号装置５４、５６と、比較判定部５５と、スイッチ５０とから構成される。このような構成によれば、図５に示す構成と比較して復号装置５４、５６での復号処理が同時に行われるので、処理が高速であるという利点がある。

【００８２】図７は図５に示す装置構成の他の変形例を示す図であり、暗号化装置５７と、復号装置５８と、比較判定部５９とから構成される。このような構成によれば、図６では２つの復号装置が必要になるのに対して、暗号化時の暗号化装置１０を暗号化装置５７として使用することができ、かつ、暗号化装置５７での暗号化処理と復号装置５８での復号処理が同時に行われるので処理が高速であるという利点がある。

【００８３】上記した第１、第２実施形態によれば、本発明によれば、たとえ装置が盗難されたり分解されたりしても、内部に記憶された機密情報を保護することができるようになる。また、誤ったマスター鍵による復号に起因するファイルの破壊や機密情報の漏洩を防止することができる。

【００８４】図８は、本発明の第３実施形態に係る情報処理システム（暗号側）の構成を示す図である。本実施形態に係る情報処理システムは、概略的には、暗号側となる情報処理装置において、所定の一時鍵を生成し、これを用いて暗号化対象となるデータを暗号化するとともに、この一時鍵の暗号化を、マスタ鍵を記憶している処理機能付き外部記憶装置に依頼し、処理機能付き外部記憶装置において、受け取った一時鍵に対し、自装置内に記憶されている所定のマスタ鍵を用いた所定の暗号化を施して、情報処理装置に暗号化鍵を戻すものである。

【００８５】また、外部記憶装置の内部で一時鍵を発生させることも可能である。このようにすれば情報処理装置との間のデータ転送回数を減らすことができる。同様に、本実施形態に係る情報処理システムは、概略的には、復号側となる情報処理装置において、暗号化データに含まれる一時鍵とマスタ鍵をもとにした暗号化鍵の復号化を、マスタ鍵を記憶している処理機能付き外部記憶装置に依頼し、処理機能付き外部記憶装置において、受け取った暗号化鍵の情報と自装置内に記憶されている所定のマスタ鍵をもとに、所定の復号化を行って、もとの一時鍵を取り出し、これを情報処理装置に戻し、情報処理装置において、渡された一時鍵を用いて、暗号化されたデータを復号するものである。

【００８６】各情報処理装置は、単一ユーザであっても、複数ユーザで共用するものであっても良い。ただし、後述するマスタ鍵を保管した処理機能付き外部記憶装置は、ユーザ毎に容易するのが望ましい。

【００８７】本実施形態では、あるデータａを鍵Ｋを用いて暗号化する操作をE_K （ａ）と表現し、あるデータａを鍵Ｋを用いて復号化する操作をD_K （ａ）と表現する。この表現を用いることにより、例えば、あるデータａを鍵Ｋ１を用いて暗号化し鍵Ｋ２を用いて復号する操作は、D_{K2}（E_{K1}（ａ））で表される。

【００８８】なお、本実施形態では、暗号化対象となるデータの暗号方式と、このデータの暗号化や復号化に使用する一時鍵の暗号方式には、ＤＥＳあるいはＦＥＡＬ

などの所望の共通鍵暗号方式を用いるものとする。なお、前者の処理対象データの暗号方式と後者の一時鍵の暗号方式とは同一であっても良いし、相違するものであっても良い。

【００８９】ここで、暗号化の対象となるデータは、例えば、文書、音声、画像、プログラムなどである。その他にも、種々のもの形態が考えられる。また、本実施形態では、復号化の対象となる暗号化データは、暗号化された鍵の情報を含むヘッダ部と、暗号化されたデータを含むデータ部からなるものとする。例えば、ファイルあるいはパケット、セルといったものがこれに該当する。

【００９０】以下では、暗号側の情報処理システムと復号側の情報処理システムを順に説明する。なお、本発明を情報処理装置に適用する場合、暗号側の構成のみを持っても良いし、復号側の構成のみを持っても良いし、両方を兼ね備えても良い。同様に、本発明を処理機能付き外部記憶装置に適用する場合、暗号側の構成のみを持っても良いし、復号側の構成のみを持っても良いし、両方を兼ね備えても良い。

【００９１】なお、平文のデータをＤａｔａ、一時鍵をS_k、マスタ鍵をM_k、一時鍵で暗号化されたデータをE_{Sk}（Data）、マスタ鍵で暗号化された一時鍵をE_{Mk}（S_k）と、一時鍵で暗号化された一時鍵をE_{Sk}（S_k）などと表すものとする。

【００９２】まず、暗号側の情報処理システムについて説明する。図８は、本発明の第３実施形態に係る情報処理システムにおいて、暗号化を行う側の情報処理装置１０１と外部記憶装置１０２の構成を示す図である。

【００９３】ここで、情報処理装置１０１は第１実施形態の携帯型ＰＣ６に、外部記憶装置１０２はＩＣカード５に、一時鍵生成部１０５は乱数生成部３に、暗号化部１０４、１０８は暗号化装置４、１０に、暗号化データ生成部１０６は記憶装置１０に対応している。

【００９４】情報処理装置１０１は、一時鍵の生成やデータの暗号化などを行うものである。情報処理装置１０１には、例えば、パーソナルコンピュータを用いることができる。

【００９５】外部記憶装置１０２は、マスター鍵の保管、一時鍵の暗号化などを行うものである。外部記憶装置１０２には、例えば、処理機能を有するＩＣカードを用いることができる。

【００９６】情報処理装置１０１と外部記憶装置１０２とは、それぞれの持つインタフェース部（図示せず）を介して、データの受け渡しを行う。例えば、使用時に外部記憶装置１０２を情報処理装置１０１内のソケットに直接接続する方法を用いても良いし、赤外線などにより通信できるようにしても良い。

【００９７】なお、外部記憶装置１０２を使用しないときは、これをユーザが安全な場所に保管しておくのが好ましい。さて、図８に示すように、データの暗号化を行

う側の情報処理装置１０１は、平文ラ
３、暗号化部１０４、一時鍵生成部１
タ生成部１０６を備えている。

【００９８】平文データ保持部１０３
なる平文のデータを保持するためのも
の対象であるデータは、所定の記憶装
のでも良いし、有線や無線の通信回線
ものでも良いし、当該情報処理装置」
したものであっても良いし、映像機器
ら直接当該情報処理装置に取り込んだ
い。

【００９９】一時鍵生成部１０５は、
１０３に保持されたデータを暗号化す
時鍵を生成する。また、一時鍵生成部
ない乱数発生器により生成された乱数
ともデータ毎に一時鍵を生成する。乱
器は、例えば所定のタイミングで時計
得た時間情報をもとにして乱数を生成
良い。さらに、一時鍵は、同じデータ
暗号化する度に異なる鍵を生成し使用
い。なお、乱数発生器は、情報処理装
ても良いし、外部記憶装置１０２側に

【０１００】なお、この一時鍵は、
介して外部記憶装置１０２にも渡され
４は、一時鍵生成部１０５で生成され
て、平文データ保持部１０３に保持さ
化する。

【０１０１】暗号化データ生成部１０
置１０２からインタフェース部を介し
は複数の所定のマスタ鍵をそれぞれ使
た一時鍵と、一時鍵自身で暗号化され
ヘッダ部１６１に含み、暗号化部１０
た一時鍵で暗号化されたデータをデー
暗号化データを生成する。なお、暗号
０６が暗号化データを作成した時点で
タは削除されるものとする。

【０１０２】暗号化により得られた時
えば、この情報処理装置１０１の内蔵
の記憶装置あるいはフロッピーディス
などのリムーバブルな記憶媒体に格納
ＡＮを介してファイル管理装置等に転
有線や無線の通信回線を介して所望の
送先（復号側となる情報処理装置）に

【０１０３】ここで、マスタ鍵の管理
すべてのマスタ鍵を個人用マスタ鍵と
マスタ鍵とグループで共有するグルー
する方法など、種々の方法が考えられ
用マスタ鍵とグループで共有するグル
入する場合、０、１または複数の個人
化した一時鍵、０、１または複数のグ

時鍵自身で暗号化した一時鍵を、
部に付加することになる。この場
ッダ部は可変長で使用すれば良

時鍵の暗号化に使用可能なマスタ
て、ヘッダ部を固定長で使用して
の暗号化を行う側の外部記憶装置
る。

記憶装置１０２は、マスタ鍵の情
つとともに、このマスタ鍵のデー
に出さずに、情報処理装置１０１
暗号化処理を全て自装置内で行っ
処理装置１に返す働きを持つもの

すように、一時鍵の暗号化を行う
２は、マスタ鍵記憶部１０９、暗
いる。マスタ鍵記憶部１０９は、
鍵の情報を記憶する。

タ鍵記憶部１０９は、自装置外部
みなどのアクセスを不可とするの
パスワード・チェックなどの認証
鍵の情報の追加、削除などの操作
ても良い。

１０８は、インタフェース部を介
１から送信された一時鍵を受け取
定のマスタ鍵を用いて一時鍵を暗
の一時鍵を、一時鍵自身で暗号化

外部記憶装置１０２の暗号化部１
を示す。なお、図９の暗号化部１
とは、独立に設けても良いし、１
えて使用するようにしても良い。
複数のマスタ鍵でそれぞれ暗号化
時鍵自身で暗号化された一時鍵
を介して情報処理装置１０１に送
生成部１０６により暗号化データ
納される。

、外部記憶装置１０２内での一時
スタ鍵の指定方法には、例えば次
れる。

１０９に記憶されているすべての
とし、それぞれのマスタ鍵毎に、
た一時鍵を生成する。

スタ鍵記憶部１０９に記憶されて
用するものを、情報処理装置１０
記憶装置１０２側では、指定され
スタ鍵で暗号化された一時鍵を生
例を図１０と図１１に示す。例え
２内のマスタ鍵記憶部１０９に、
ＩＤと鍵データとユーザ情報（例

えば、
Ｄ）と
置１０
部１０
データ
表示装
２２２
ープ名
ウ２２
アイコ
するな
択指示
ＤおよＤ
情報処
その後
照して
を用い
【０１
部記憶
を含む
ユーザ
法が考
【０１
を示す
１０５
暗号化
された
て、暗
ップＳ
【０１
生成さ
文のデ
３）。
０２に
置１０
は複数
スター
【０１
１２も
外部記
Ｓｋと
１５）
E_{Mki}
６）、
ｋ）を
【０１
した
鍵記憶
（２）
置１０

のである。

【０１１８】次に、これらE_{Mki}（S_k）とE_{Sk}（S_k）を、情報処理装置１０１に送信する（ステップＳ１８）。情報処理装置１０１側では、これらE_{Mki}（S_k）とE_{Sk}（S_k）を受信すると（ステップＳ１９）、暗号化データ生成部６により、E_{Mki}（S_k）とE_{Sk}（S_k）をヘッダ部に含み、E_{Sk}（Data）をデータ部とするファイルやパケットなどの暗号化データを作成する（ステップＳ２０）。

【０１１９】以上のようにして生成された暗号化データは、所定の記憶装置に保存され、あるいはネットワークなどを介して所望の宛先装置（復号側となる情報処理装置）に転送される。

【０１２０】ここで、暗号化されたデータE_{Sk}（Data）を解読するためには、E_{Mki}（S_k）を解読して一時鍵を取り出す必要があるので、復号側で該当するマスタ鍵を所有する場合にのみデータＤａｔａを取り出すことができる。例えば、M_{k1}、M_{k2}、M_{k3}をそれぞれ用いて一時鍵S_kを暗号化した場合、暗号化データのヘッダ部には、E_{Mk1}（S_k）、E_{Mk2}（S_k）、E_{Mk3}（S_k）が含まれるので、M_{k1}、M_{k2}、M_{k3}のいずれかのマスタ鍵を持つものが、平文のデータＤａｔａを得ることができる。なお、言うまでもなく、ヘッダ部の情報から一時鍵やマスタ鍵を解読するのはきわめて困難である。

【０１２１】また、復号側では、ヘッダ部に含まれる一時鍵自身で暗号化された一時鍵E_{Sk}（S_k）をもとにして、復号した一時鍵の検証を行うことができる。さらに、１つの暗号化データを解読可能とするマスタ鍵の数にかかわらず、上記検証のために付加する情報は、一時鍵自身で暗号化された一時鍵のただ１つのみで良く、マスタ鍵の個数に相当する回数の一時鍵の暗号化と１回だけの一時鍵自身の暗号化を行うことにより、全てのマスタ鍵に対する検証を施すことができるので、同一データに対する複数のマスタ鍵の使用が容易になる。

【０１２２】例えば、各々のマスタ鍵で一時鍵を１回暗号化したものと２回暗号化したものを組にしてヘッダに格納し、復号化の際、同じマスタ鍵で同じ一時鍵を１回と２回復号化した２種類の一時鍵の一致判定を行うことにより、マスタ鍵の検証を行うこともできる。しかし、この方法によると、ヘッダに格納する暗号化された一時鍵の情報は、マスタ鍵の個数の２倍に相当するサイズになる。これに対して、上記の各々のマスタ鍵による一時鍵の暗号化と一時鍵自身による一時鍵の暗号化では、マスタ鍵の個数＋１に相当する情報だけをヘッダに格納することができ、ヘッダサイズを小さく抑えることができる。

【０１２３】なお、一時鍵は少なくともデータ毎に生成されるので、たとえある暗号化データの一時鍵が解読されたとしても、他の暗号化データをその一時鍵で解読することはできない。

【０１２４】次に、復号側の情報処理システムについて説明する。図１４は、本発明の一実施形態に係る情報処理システムにおいて、復号化を行う側の情報処理装置１１１と外部記憶装置１１２の構成を示す図である。

【０１２５】情報処理装置１１１は、データの復号化などを行うものである。情報処理装置１１１には、例えば、パーソナルコンピュータを用いることができる。外部記憶装置１１２は、マスター鍵の保管、一時鍵の復号などを行うものである。外部記憶装置１１２には、例えば、処理機能を有するＩＣカードを用いることができる。

【０１２６】情報処理装置１１１と外部記憶装置１１２とは、それぞれの持つインタフェース部（図示せず）を介して、データの受け渡しを行う。例えば、使用時に外部記憶装置１１２を情報処理装置１１１内のソケットに直接接続する方法を用いても良いし、赤外線などにより通信できるようにしても良い。

【０１２７】なお、外部記憶装置１１２を使用しないときは、これをユーザが安全な場所に保管しておくのが好ましい。さて、図１４に示すように、復号を行う側の情報処理装置１１１は、暗号化データ保持部１１６、復号化部１１４、復号化データ保持部１１３を備えている。

【０１２８】暗号化データ保持部１１６は、復号化対象となる暗号化データを保持するためのものである。復号化の対象である暗号化データは、所定の記憶装置から読出したものでも良いし、有線や無線の通信回線を介して取得したものでも良い。

【０１２９】ここで、暗号化データ保持部１１６に保持されている暗号化データのヘッダ部に含まれるマスタ鍵で暗号化された一時鍵と一時鍵自身で暗号化された一時鍵の情報は、インタフェース部を介して外部記憶装置１１２に渡される。なお、外部記憶装置１１２にヘッダ部全体を送信するようにしても良い。

【０１３０】また、上記暗号化データのデータ部に含まれる一時鍵で暗号化されたデータは、復号化部１１４に渡される。復号化部１１４では、外部記憶装置１１２からインタフェース部を介して返された一時鍵を用いて、上記の一時鍵で暗号化されたデータを復号化する。

【０１３１】復号化データ保持部１１３は、この復号化により得られた平文のデータを保持するためのものである。なお、復号化により得られたデータは、例えば、ＣＲＴや液晶などの表示装置に表示され、あるいは画像や音声の再生装置に出力され、あるいはこの情報処理装置１１１の内蔵ハードディスク等の記憶装置あるいはフロッピーディスクやＣＤ－ＲＯＭなどのリムーバブルな記憶媒体にファイルとして格納され、あるいはＬＡＮを介してファイル管理装置に転送され、あるいはパケットやセルの形にして有線や無線の通信回線を介して所望の転送先に送り出される。

【０１３２】次に、一時鍵の復号化を行う側の外部記憶

装置１１２について説明する。この外部記憶装置１１２は、マスタ鍵の情報を保管する機能を持つとともに、このマスタ鍵のデータ自体を自装置の外部に出さずに、情報処理装置１１１から渡された所定のマスタ鍵で暗号化された一時鍵の情報をもとに復号化処理を全て自装置内で行ってその結果得られた一時鍵（または復号不可を示す制御信号）を情報処理装置１１１に返す働きを持つものである。

【０１３３】図１４に示すように、一時鍵の復号化を行う側の外部記憶装置１１２は、マスタ鍵記憶部１１９、復号化部１１８を備えている。マスタ鍵記憶部１１９は、１または複数のマスタ鍵を記憶する。

【０１３４】このマスタ鍵記憶部１１９は、自装置外部からの読出しや書き込みなどのアクセスを不可とするのが望ましい。ただし、パスワード・チェックなどの認証に通過すれば、マスタ鍵の情報の追加、削除などの操作が可能となるようにしても良い。

【０１３５】復号化部１１８は、インタフェース部を介して情報処理装置１１１から送信されたマスタ鍵で暗号化された一時鍵および一時鍵自身で暗号化された一時鍵を受け取り、マスタ鍵記憶部１１９内に記憶されているマスタ鍵を用い復号化を行って、平文の一時鍵を得ることと、鍵の検証とを同時に行う。

【０１３６】図１５は、本発明の第４実施形態に係る鍵の判定を実現するための鍵判定システムの構成を示す図である。１または複数のマスタ鍵でそれぞれ暗号化された一時鍵および一時鍵自身で暗号化された一時鍵が、インタフェース部を介して情報処理装置１１１から送信されると、復号化部２８１にて、マスタ鍵記憶部１１９に格納されているマスタ鍵を用いて、マスタ鍵で暗号化された一時鍵を復号する。この復号化された一時鍵を用いて、復号化部２８２にて、一時鍵自身で暗号化された一時鍵を復号する。そして、２つの一時鍵が一致するか否かを一致判定部２８３により判定する。２つの一時鍵が一致しないならば、マスタ鍵記憶部１１９に記憶された他のマスタ鍵を用いて、上記と同様に復号と判定を行う。

【０１３７】もし一時鍵の一致判定が成功したならば一致判定部２８３はゲート回路２８４を閉じ、一時鍵は、外部記憶装置１１２からインタフェース部を介して情報処理装置１１１に送信される。この場合、上記のように情報処理装置１１１内の復号化部１１４にてこの一時鍵を用いて復号が行われる。

【０１３８】もし、この外部記憶装置１１２内のマスタ鍵記憶部１１９に記憶された全マスタ鍵について一時鍵の一致判定に失敗したならば、この外部記憶装置１１２ではこの暗号化された一時鍵を解くことはできない。この場合、一致判定部２８３はその旨を示す制御信号を発し、これが外部記憶装置１１２からインタフェース部を介して情報処理装置１１１に送信される。もちろん、この場合、一時鍵は、情報処理装置１１１に送信されず、情報処理装置１１１では、暗号化データを復号化することはできない。

【０１３９】なお、図１５の復号化部２８１と復号化部２８２とは、独立に設けても良いし、１つの復号化部を切り換えて使用するようにしても良い。図１６は鍵の判定動作手順の一例を示すフローチャートである。

【０１４０】情報処理装置１１１側では、まず暗号化データ保持部１１６に格納されている暗号化データのヘッダ部１６１に含まれるE_{Mki}（S_k）とE_{Sk}（S_k）を、外部記憶装置１１２に送信する（ステップＳ２１）。

【０１４１】外部記憶装置１１２側では、このE_{Mki}（S_k）とE_{Sk}（S_k）を受信する（ステップＳ２２）。なお、情報処理装置１１１側からヘッダ部１６１全体を送信するようにした場合には、ヘッダ部１６１からE_{Mki}（S_k）とE_{Sk}（S_k）を取り出す。

【０１４２】次に、情報処理装置１１１から渡されたE_{Mki}（S_k）と、マスタ鍵記憶部１１９に記憶されているマスタ鍵M_{kj}の組を選択する（ステップＳ２３）。次に、マスタ鍵M_{kj}を用いて、復号化部２８１にて、暗号化された一時鍵E_{Mki}（S_k）を復号して$S_k' = D_{Mkj}$（E_{Mki}（S_k））を求める（ステップＳ２４）。

【０１４３】次に、この$S_k' = D_{Mkj}$（E_{Mki}（S_k））を用いて、復号化部２８２にて、マスタ鍵で暗号化されたE_{Sk}（S_k）を復号して$S_k'' = D_{Sk'}$（E_{Sk}（S_k））を求める（ステップＳ２５）。

【０１４４】次に、一致判定部２８３にて、S_k'とS_k''を比較し、一致しない場合（ステップＳ２６）、情報処理装置１１１から渡されたE_{Mki}（S_k）と、マスタ鍵記憶部１１９に記憶されているマスタ鍵M_{kj}の組でまだ選択していないものがあれば、（ステップＳ２７）、ステップＳ２３に戻る。

【０１４５】もし一致判定部２８３にてS_k'とS_k''を比較し、一致した場合（ステップＳ２６）、得られた一時鍵S_k（$= S_k' = S_k''$）を、情報処理装置１１１に送信する（ステップＳ２８）。

【０１４６】情報処理装置１１１側では、一時鍵S_kを受信すると（ステップＳ２９）、暗号化されたデータE_{Sk}(Data)を一時鍵S_kで復号して平文のデータＤａｔａを取り出す（ステップＳ３０）。

【０１４７】なお、情報処理装置１１１から渡されたE_{Mki}（S_k）と、マスタ鍵記憶部１１９に記憶されているマスタ鍵M_{kj}の組すべてについてステップＳ２３～Ｓ２６までの処理を試行し、そのすべてにおいて$S_k' = S_k''$が得られなかった（ステップＳ２６でＮｏとなった）場合、暗号化に使用したマスタ鍵が存在しないために一時鍵を復号化できなかった旨を示す制御信号を情報処理装置１１１に送信する。

【０１４８】なお、図１７に、鍵判定システムの他の構

成を示す。図１５との相違は、マスタ鍵M_{kj}でE_{Mki}（S_k）を復号して$S_k'=D_{Mkj}$（E_{Mk}（S_k））を求め、このS_k'をS_k'自身で暗号化してE_{Sk}'（S_k'）を求め、E_{Mki}（S_k）とE_{Sk}'（S_k'）の一致により検証を行う点である。この処理手順のフローチャートは、図１６のステップＳ２５の処理で、S_k'をS_k'自身で暗号化してE_{Sk}'（S_k'）を求める点、ステップＳ２６でE_{Mki}（S_k）とE_{Sk}'（S_k'）を比較する点以外は、図１６と同様である。

【０１４９】なお、図１７の復号化部２８１と暗号化部２８５の処理が同内容になる暗号方式を採用する場合、復号化部２８１と暗号化部２８５とは、独立に設けても良いし、１つの回路を切り換えて使用するようにしても良い。

【０１５０】前述したように、暗号化されたデータE_{Sk}(Data)を解読するためには、E_{Mki}（S_k）を解読して一時鍵を取り出す必要があるので、復号側で該当するマスタ鍵を所有する場合にのみデータＤａｔａを取り出すことができる。例えば、暗号化データのヘッダ部にE_{Mk1}（S_k）、E_{Mk2}（S_k）、E_{Mk3}（S_k）が含まれる場合には、M_{k1}、M_{k2}、M_{k3}のいずれかのマスタ鍵を持つものが、平文のデータＤａｔａを得ることができる。

【０１５１】つまり、このＤａｔａをM_{k1}、M_{k2}、M_{k3}のいずれかのマスタ鍵を持つユーザによって共有し、他のユーザには内容を秘匿することができる。また、ヘッダ部に含まれる一時鍵自身で暗号化された一時鍵E_{Sk}（S_k）をもとにして、復号した一時鍵の検証を行い、検証を通過しない場合には復号化の処理が実行されないので、異なる鍵を用いて誤って暗号化されたデータを破壊するようなトラブルを回避することができる。

【０１５２】さらに、１つの暗号化データを解読可能とするマスタ鍵の数にかかわらず、上記検証のために不可する情報は、一時鍵自身で暗号化された一時鍵のただ１つのみで良いという利点がある。

【０１５３】また、以上のような本実施形態によれば、一時鍵の暗号化、復号化は、情報処理装置の外部で行われるため、マスタ鍵と情報処理装置が分離され、マスタ鍵を安全に扱うことができる。例えば、不正な第３者が本情報処理装置にアクセスしたとしてもても、マスタ鍵は情報処理装置内には存在しないので、マスタ鍵を盗用されることはない。

【０１５４】また、データの暗号化および復号化は、暗号化する度に生成される一時鍵を用いて行うので、ある暗号化データの一時鍵が解読された場合でも、他の暗号化データをその一時鍵で解読することはできない。

【０１５５】また、データを暗号化する一時鍵を変更せずに、マスタ鍵だけを変更する場合、ヘッダ部に所望のマスタ鍵で暗号化した一時鍵を追加し、あるいはヘッダ部から該当するマスタ鍵で暗号化した一時鍵を削除すれば良く、データを再暗号化する必要がない。

【０１５６】また、暗号方式として任意の方式を用いる場合、暗号方式の識別子を暗号化データのヘッダ部に付加しておけば、暗号方式を自由に選択することが可能である。

【０１５７】なお、暗号側で用いる処理機能付き外部記憶装置１と復号側で用いる処理機能付き外部記憶装置１１とを１つの外部記憶装置で共用する場合、暗号化に用いるマスタ鍵と復号化に用いるマスタ鍵を同一にしても良いし、暗号化にのみ使用可能なマスタ鍵記憶部と復号化にのみ使用可能なマスタ鍵記憶部を設け、それぞれに所望のマスタ鍵を記憶させるようにしても良い。

【０１５８】ここで、本実施形態に係る情報処理システムの利用例について述べる。例えば、前述した暗号側と復号側の機能を兼ね備える情報処理装置を複数台、ＬＡＮなどに接続する。また、このＬＡＮにはファイルを蓄積・管理するするファイル管理装置が接続されているものとする。各情報処理装置のユーザは、前述のようにマスタ鍵を保管してある処理機能付き外部記憶装置を用いて、暗号化されたーデータを含むファイルを作成し、ＬＡＮを介して上記のファイル管理装置に保存する。その際、そのファイルのヘッダに所望のユーザのマスタ鍵により暗号化された一時鍵を付加しておけば、当該暗号化ファイルは、該当するユーザであればいずれも解読することができる。このようにして、暗号化ファイルを安全に共有するシステムを構築することができる。

【０１５９】もちろん、１つのスタンドアローンの情報処理装置を複数ユーザで共用しており、この情報処理装置に内蔵のハードディスク装置に格納されるファイルを複数ユーザで共有するような場合にも、本発明は適用可能である。

【０１６０】ところで、暗号化対象であるデータの暗号方式と一時鍵の暗号方式の少なくとも一方に、ＲＳＡなどの所望の公開鍵暗号方式を用いても良い。例えば、一時鍵の暗号方式に所望の公開鍵暗号方式を用いる場合、暗号化する際、マスタ鍵として対象ユーザの公開鍵を使用し、復号化する際、マスタ鍵として自身の秘密鍵を使用する。また、例えば、暗号化対象であるデータの暗号方式に、暗号化鍵と復号化鍵が異なる暗号方式を用いる場合、暗号化する際、一時鍵として暗号化鍵と復号化鍵の対を生成し、暗号化鍵でデータを暗号化するとともに、復号化鍵を暗号化し、これをヘッダ部に格納する。

【０１６１】また、マスタ鍵を格納する外部記憶装置を使用しないならば、以下のようにマスタ鍵を生成し使用する。まず、暗号化、復号化を行う情報処理装置にパスワードやＩＤ番号を入力することにより、一方向性関数等を用いて、暗号化、復号化の鍵を生成するマスタ鍵生成部を用意する。このマスタ鍵生成部では、個人やグループのパスワードやＩＤ番号を入力することにより、異なるマスタ鍵を各々に対し生成する。これらのマスタ鍵

は、上記した方法と同じように、暗号化装置では一時鍵を暗号化するときに使用し、復号化装置では一時鍵を復号するときに使用する。

【０１６２】以上の各構成は、ハード・ワイヤードで形成することも、相当するプログラムをＣＰＵで実行させる形で実現することも可能である。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０１６３】以上、上記した第３、第４実施形態によれば、所定の一時鍵で暗号化されたデータに、所定のマスタ鍵で暗号化された一時鍵と、一時鍵自身で暗号化された一時鍵を付加するので、該当するマスタ鍵を持つユーザのみ鍵の検証と暗号化されたデータの復号化を行うことができ、その他のユーザには内容を秘匿することができる。

【０１６４】また、一時鍵自身で暗号化した一時鍵を用いて鍵の検証を行いながら復号化を行うので、正当ではないマスタ鍵の誤用などによる復号時のデータの破壊を避けることができる。しかも、一時鍵自身で暗号化された一時鍵を付加するだけで、すべてのマスタ鍵について鍵の検証を行うことができる。

【０１６５】従って、例えば、個人やグループなどの複数のユーザで共有するデータを、暗号化した形で安全に保存できるようになる。また、一時鍵の暗号化、復号化は、情報処理装置の外部で行われるため、マスタ鍵と情報処理装置が分離され、マスタ鍵を安全に扱うことができる。例えば、不正な第３者が本情報処理装置にアクセスしたとしても、マスタ鍵は情報処理装置内には存在しないので、マスタ鍵を盗用されることはない。

【０１６６】図１８は、本発明の第５実施形態として、鍵の判定方法を一般化した場合の鍵判定システムの構成を示す図である。第５実施形態に係る鍵判定システムでは、一時鍵S_kをマスター鍵M_kで暗号化して得られるデータをM_k（S_k）として入力するとともに、後述する複数のチェック関数の任意の一つをチェックデータとして選択的に入力する。判定部３００はこれら２つのデータに基づいて、マスター鍵を用いた所定の暗号化及び／または復号処理を行なうことにより、当該マスター鍵が正しいか否かを判定し、この判定結果（ＹＥＳ／ＮＯ）を出力するとともに、復号された一時鍵S_kを出力する。

【０１６７】図１９は鍵判定システムに対する入力となり得る複数のチェック関数を区分けして示すテーブルを示すものである。チェック関数Ｘ（ａ）とは鍵ａを鍵Ｘで暗号化して得られるデータを意味し、X^{-1}（ａ）は鍵ａを鍵Ｘで復号して得られるデータを意味し、X^2（ａ）は鍵ａを鍵Ｘで２回暗号化して得られるデータを意味する。また、ｈはハッシュ関数を意味し、｜｜は２つの鍵を並べることを意味し、＋は加算を意味し、ｄは複数の人によって共有される共有データであり、d^*は時変、すなわち、暗号化あるいは復号処理を行なう毎に異なる共有データを表す。

【０１６８】まず、M_kの暗号化あるいは復号を行なう場合に用いられる各チェック関数について説明する。チェック関数がM_kとS_kを共に含む場合は、S_k（M_k）とS_k^{-1}（M_k）が存在し、いずれも含まない場合はｈ（M_k｜｜S_k）が存在する。また、チェック関数がM_kのみか、あるいはM_kと他のデータを含む場合には、M_k（M_k）、M_k^{-1}（M_k）、M_k（M_k＋d^*）、M_k^{-1}（M_k＋d^*）の４通りが存在し、含まない場合はM_k（d^*）、M_k^{-1}（d^*）、ｈ（M_k）の３通りが存在する。また、チェック関数がS_kのみか、あるいはS_kと他のデータについてのチェック関数は存在しない。

【０１６９】次に、S_kの暗号化あるいは復号を行なう場合に用いられる各チェック関数について説明する。チェック関数がM_kとS_kを共に含む場合は、M_k^2（S_k）とM_k^{-1}（S_k）が存在し、含まない場合はｈ（M_k｜｜S_k）が存在する。また、チェック関数がM_kのみか、あるいはM_kと他のデータについてのチェック関数は存在しない。また、チェック関数がS_kのみか、あるいはS_kと他のデータを含む場合はS_k（S_k）、S_k^{-1}（S_k）が存在し、含まない場合はS_k（ｄ）、S_k^{-1}（ｄ）、ｈ（S_k）の３通りが存在する。

【０１７０】図２０は、チェック関数として、S_k（M_k）が入力される場合の鍵判定システムの構成を示す図であり、復号回路３０１と暗号化回路３０２と一致判定部３０３とゲート３０４とを具備する。復号回路３０１、暗号化回路３０２、一致判定部３０３の動作は前記した通りである。矢印はマスター鍵M_kの入力を意味する。また、ゲート３０４はデータを出力するかどうかを制御するのに用いられる。これらの説明は以下で述べるチェック関数にも適用されるものとする。

【０１７１】図２１は、チェック関数として、S_k^{-1}（M_k）が入力される場合の鍵判定システムの構成を示す図であり、復号回路３０５、３０６と、一致判定部３０７と、ゲート３０８を具備する。

【０１７２】図２２は、チェック関数として、M_k（M_k）が入力される場合の鍵判定システムの構成を示す図であり、復号回路３０９と一致判定部３１０と暗号化回路３１１とゲート３１２とを具備する。

【０１７３】図２３は、チェック関数として、M_k^{-1}（M_k）が入力される場合の鍵判定システムの構成を示す図であり、ゲート３１３と復号回路３１４と一致判定部３１５と復号回路３１６とを具備する。

【０１７４】図２４は、チェック関数として、d^*及びM_k（M_k＋d^*）が入力される場合の鍵判定システムの構成を示す図であり、ゲート３１７と復号回路３１８と一致判定部３１９と暗号化回路３２０と加算回路３２１とを具備する。

【０１７５】図２５は、チェック関数として、d^* 及び M_k^{-1}（$M_k + d^*$）が入力される場合の鍵判定システムの構成を示す図であり、ゲート３２２と復号回路３２３と一致判定部３２４と復号回路３２５と加算回路３２６とを具備する。

【０１７６】図２６は、チェック関数として、h（$M_k || S_k$）が入力される場合の鍵判定システムの構成を示す図であり、復号回路３２７と連結部３２８とハッシュ関数（h）３２９とゲート３３０と一致判定部３３１とを具備する。

【０１７７】図２７は、チェック関数として、d^* 及び M_k（d^*）が入力される場合の鍵判定システムの構成を示す図であり、復号回路３３２と一致判定部３３３とゲート３３４と復号回路３３５とを具備する。

【０１７８】図２８は、チェック関数として、d^* 及び M_k^{-1}（d^*）が入力される場合の鍵判定システムの構成を示す図であり、暗号化回路３３６と一致判定部３３７とゲート３３８と復号回路３３９とを具備する。

【０１７９】図２９は、チェック関数として、h（M_k）が入力される場合の鍵判定システムの構成を示す図であり、一致判定部３４０とハッシュ関数（h）３４１とゲート３４２と復号回路３４３とを具備する。

【０１８０】図３０は、チェック関数として、M_k^2（S_k）が入力される場合の鍵判定システムの構成を示す図であり、復号回路３４４と暗号化回路３４５とゲート３４７と一致判定部３４６とを具備する。

【０１８１】図３１は、チェック関数として、M_k^{-1}（S_k）が入力される場合の鍵判定システムの構成を示す図であり、復号回路３４８と一致判定部３４９と暗号化回路３５０とを具備する。

【０１８２】図３２（ａ）、（ｂ）は、チェック関数として、S_k（S_k）が入力される場合の鍵判定システムの構成を示す図である。図３２Ａは復号回路３６０と暗号化回路３６１と一致判定部３６２とゲート３６３とを具備し、図３２Ｂは復号回路３６４、３６５と一致判定部３６６とゲート３６７とを具備する。

【０１８３】図３３（ａ）、（ｂ）は、チェック関数として、S_k^{-1}（S_k）が入力される場合の鍵判定システムの構成を示す図である。図３３Ａは復号回路３６８、３６９と一致判定部３７０とゲート３７１とを具備し、図３３Ｂは復号回路３７２と暗号化回路３７３と一致判定部３７４とゲート３７５とを具備する。

【０１８４】図３４は、チェック関数として、d及びS_k（d）が入力される場合の鍵判定システムの構成を示す図であり、復号回路３７６、３７７と一致判定部３７８とゲート３７９とを具備する。

【０１８５】図３５は、チェック関数として、d及びS_k^{-1}（d）が入力される場合の鍵判定システムの構成を示す図であり、復号回路３８０と暗号化回路３８１と一致判定部３８２とゲート３８３とを具備する。

【０１８６】図３６は、チェック関数としてh（S_k）が入力される場合の鍵判定システムの構成を示す図であり、復号回路３８４とハッシュ関数（h）３８５と一致判定部３８６とゲート３８７とを具備する。

【０１８７】図３７は、第５実施形態の鍵判定システムをＤＶＤ（デジタルビデオディスク）に応用した例を説明するための図である。送信側は一時鍵Ｓｋ を複数の暗号化回路５００－１～５００－ｎの各々に入力して異なるマスター鍵M_{k1}～M_{kn}を用いて暗号化して同時に送信する。このとき、一時鍵S_k を自身の鍵S_k で暗号化したデータも同時に送信する。

【０１８８】受信側では複数の復号回路５０１－１～５０１－ｎの各々に送信時に用いたマスター鍵M_{k1}～M_{kn}を入力すればS_k が得られる。このとき、例えば復号回路５０１－３においてM_{k3}とは異なるマスター鍵M_{k3}'を用いて復号した場合はS_kとは異なる一時鍵S_k'が得られるので、比較部５０３で同じS_k'で暗号化して得られるS_k'（S_k'）を送信側から送られてきたS_k（S_k）と比較しても一致しないのでS_kが出力されずエラーとなる。このようにしてマスター鍵の真偽判定が行われる。

【０１８９】図３８は、第５実施形態の鍵判定システムを電子メールに応用した例を説明するための図である。電子メールのヘッダ４００には、一時鍵S_k を複数の異なるマスター鍵M_{k1}～M_{kn}で暗号化したデータM_{k1}（S_k）～M_{kn}（S_k）と、S_k を同じS_k で暗号化したS_k（S_k）とを記録し、ボディ４０１には、本文をS_kで暗号化したS_k（本文）を記録して、各M_{k1}～M_{kn}に対応する宛先１～ｎに同報的に送信する。ここで受信側としての宛先１は所持しているM_{k1}を用いて復号してS_kを取り出し、これを同じS_kで暗号化したものと、受信したS_k（S_k）とを比較し、一致した場合にはS_kが得られるのでこのS_kを用いて復号することにより本文を得ることができる。

【０１９０】ここで、不正な第３者が自身のマスター鍵で復号しようとしても比較結果が一致しないのでS_kを正しく復号できず本文が知られてしまうことはない。図３９は、第５実施形態の鍵判定システムをＣＡＴＶに応用した例を説明するための図である。

【０１９１】第１の例は受信側が鍵のデータベースを有している例である。送信側としての放送局６００がある特定地域の受信局に放送内容を送る場合に、この放送内容をS_k で暗号化したデータS_k（内容）と、S_k をM_k で暗号化したデータM_k（S_k）と、S_k をS_k で暗号化したデータS_k（S_k）と送信する。受信局のデコーダ６０１は複数の鍵からなる鍵データベース６０２を有しており、この鍵データベース６０２から受信したM_k に一致するものを鍵セレクト部６０３で選択して、選択された鍵を用いて復号することによりS_k を得る。次にこのS_k をS_k 自身で暗号化したものと、送られてき

たSk （Sk ）とを比較して一致したときにSk を復号回路６０４に出力する。復号回路６０４はこのSk を用いて受信したSk （内容）を復号して内容を取り出してＴＶ６０５の画面に表示する。ここで、不正な第３者が自身のマスター鍵で復号しようとしても比較結果が一致しないのでSk を正しく復号できず放送内容が見られてしまうことはない。

【０１９２】上記した構成において、鍵データベース６０２に、例えば受信局がその移転前に用いた鍵と、移転後に用いている鍵を記憶しておけば、移転した後でもその鍵が選択されるのでデコーダ６０１の構成を変更することなしに正常に内容を復号することができる。

【０１９３】次に第２の例を説明する。第２の例の基本的構成は第１の例と同様であるが、この例では送信側としての放送局６００と受信局の双方が鍵のデータベースを有している。放送局６００は鍵データベースの中から１つの鍵を選択して送信する。受信局のデコーダ６０１は鍵データベース６０２の中から対応する１つの鍵を選択して復号する。この場合、放送局６００から送信される鍵はMk 、Sk 共に送信ごとに逐次変更され、しかも、放送局６００はこの変更についての情報は受信局には送信しないようにする。このようにすれば第１の例の効果に加えて、安全性をより向上することができる。

【０１９４】次に第３の例を説明する。第３の例の基本的構成は第１の例と同じであり、この場合も受信局が鍵のデータベースを有しているものとする。ここでは、鍵が漏洩してしまって新たな鍵に変更したい場合や、現在の鍵のバージョンを新たなバージョンに変更したい場合に対処するために、あらかじめ新旧バージョンの鍵を鍵のデータベース６０２に含めておく。このようにすれば、デコーダ６０１の構成を変更することなしに、変更後の新しい鍵が送られてきても正常に復号することができる。

【０１９５】

【発明の効果】本発明によれば、たとえ装置が盗難されたり分解されたりしても、内部に記憶された機械情報を保護することができる情報処理装置、情報処理システム、情報処理方法、記録媒体、及び鍵の判定方法及び装置を提供することができる。

【０１９６】また、本発明によれば、複数のユーザで共有するデータを、効率的かつ安全に暗号化した形で保存できる情報処理装置、情報処理システム、情報処理方法、記録媒体、及び鍵の判定方法及び装置を提供することができる。

【図面の簡単な説明】

【図１】本発明の第１実施形態に係る情報処理システムが適用される携帯型情報処理システムにおいて、暗号化を行なう場合の装置構成を示す図である。

【図２】暗号化を行った後の携帯型情報処理システムの構成の変更を示す図である。

【図３】本発明の第１実施形態に係る情報処理システムが適用される携帯型情報処理システムにおいて、復号化を行なう場合の装置構成を示す図である。

【図４】本発明の第２実施形態に係る鍵の判定を実現するための鍵判定システムの構成を示す図である。

【図５】図４に示す装置構成を簡略化した構成を示す図である。

【図６】図５に示す構成の変形例を示す図である。

【図７】図５に示す構成の他の変形例を示す図である。

【図８】本発明の第３実施形態に係る情報処理システム（暗号側）の構成を示す図である。

【図９】図８の外部記憶装置の内部構成の一例を示す図である。

【図１０】マスタ鍵選択指示部を含めた情報処理システムの構成を示す図である。

【図１１】鍵情報テーブルの一例を示す図である。

【図１２】鍵選択指示用画面の一例を示す図である。

【図１３】暗号化の動作手順の一例を示すフローチャートである。

【図１４】本発明の第３実施形態に係る情報処理システム（復号側）の構成を示す図である。

【図１５】本発明の第４実施形態に係る鍵の判定を実現するための鍵判定システムの構成を示す図である。

【図１６】鍵の判定動作手順の一例を示すフローチャートである。

【図１７】鍵判定システムの他の構成を示す図である。

【図１８】本発明の第５実施形態として、鍵判定方法を一般化した場合の鍵判定システムの構成を示す図である。

【図１９】鍵判定システムに対する入力となり得る複数のチェック関数を区分けして示すテーブルである。

【図２０】チェック関数として、Sk （Mk ）が入力された場合の鍵判定システムの構成を示す図である。

【図２１】チェック関数として、S_k^{-1}（Mk ）が入力された場合の鍵判定システムの構成を示す図である。

【図２２】チェック関数として、Mk （Mk ）が入力された場合の鍵判定システムの構成を示す図である。

【図２３】チェック関数として、M_k^{-1}（Mk ）が入力された場合の鍵判定システムの構成を示す図である。

【図２４】チェック関数として、d* 及びMk （Mk ＋d* ）が入力された場合の鍵判定システムの構成を示す図である。

【図２５】チェック関数として、d* 及びM_k^{-1}（Mk ＋d* ）が入力された場合の鍵判定システムの構成を示す図である。

【図２６】チェック関数として、h（Mk ||Sk ）が入力された場合の鍵判定システムの構成を示す図である。

【図２７】チェック関数として、d* 及びMk （d* ）が入力された場合の鍵判定システムの構成を示す図であ

る。

【図２８】チェック関数として、d* 及びM_k^{-1}（d*）が入力された場合の鍵判定システムの構成を示す図である。

【図２９】チェック関数として、h（M_k）が入力された場合の鍵判定システムの構成を示す図である。

【図３０】チェック関数として、M_k^2（S_k）が入力された場合の鍵判定システムの構成を示す図である。

【図３１】チェック関数として、M_k^{-1}（S_k）が入力された場合の鍵判定システムの構成を示す図である。

【図３２】チェック関数として、S_k（S_k）が入力された場合の鍵判定システムの構成を示す図である。

【図３３】チェック関数として、S_k^{-1}（S_k）が入力された場合の鍵判定システムの構成を示す図である。

【図３４】チェック関数として、d及びS_k（d）が入力された場合の鍵判定システムの構成を示す図である。

【図３５】チェック関数として、d及びS_k^{-1}（d）が入力された場合の鍵判定システムの構成を示す図である。

【図３６】チェック関数としてh（S_k）が入力された場合の鍵判定システムの構成を示す図である。

【図３７】本発明の第５実施形態の鍵判定システムの第１の応用例を説明するための図である。

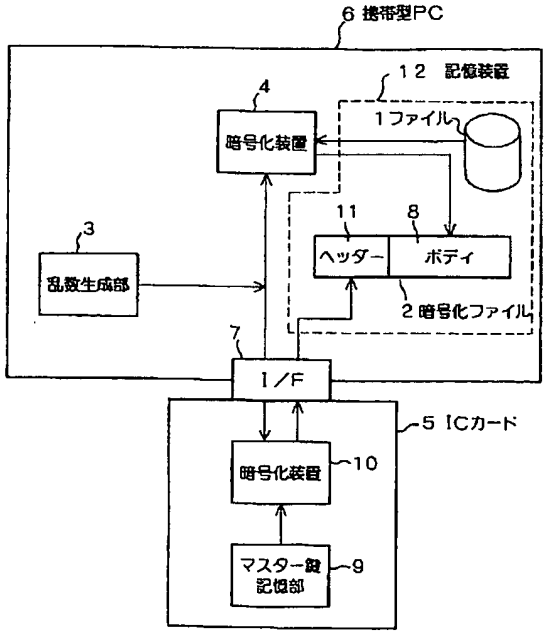
【図３８】本発明の第５実施形態の鍵判定システムの第２の応用例を説明するための図である。

【図３９】本発明の第５実施形態の鍵判定システムの第３の応用例を説明するための図である。

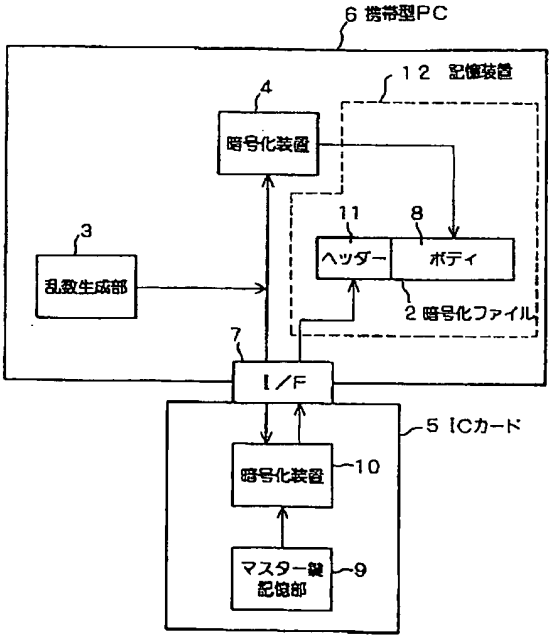
【符号の説明】

１…ファイル、２…暗号化ファイル、３…乱数生成部、４…暗号化装置、５…ＩＣカード、６…携帯型ＰＣ、７…Ｉ／Ｆ、８…ボディ、９…マスター鍵記憶部、１０…暗号化装置、１１…ヘッダー、１２…記憶装置。

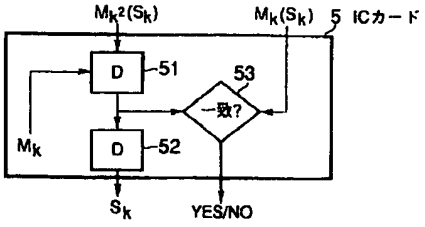
【図１】



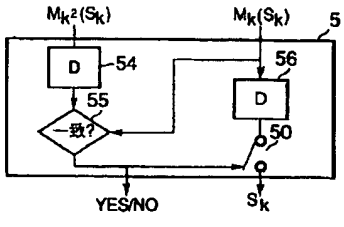
【図２】



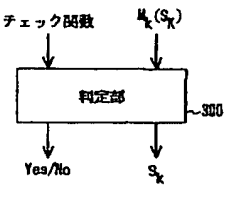
【図５】



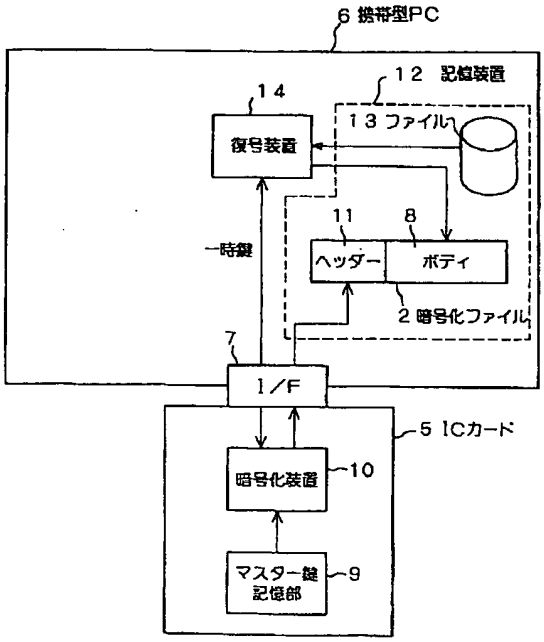
【図６】



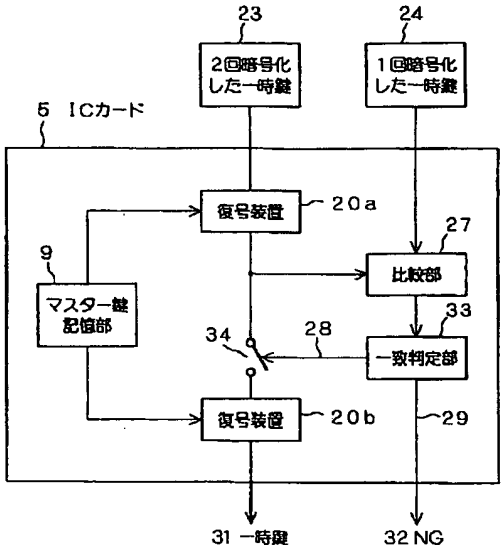
【図１８】



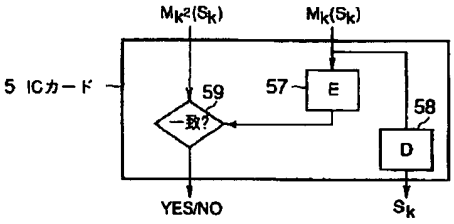
【図３】



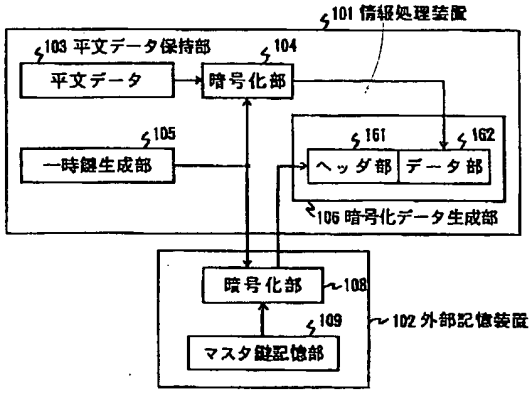
【図４】



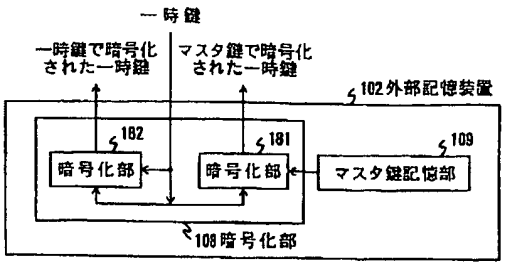
【図７】



【図８】



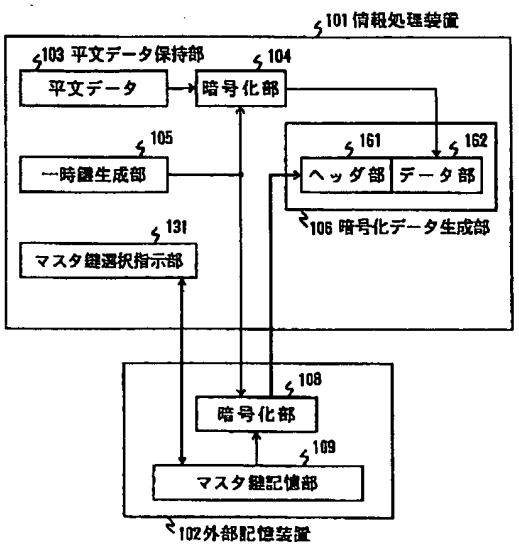
【図９】



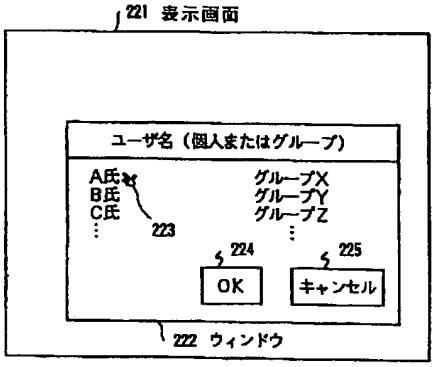
【図１１】

鍵ＩＤ	鍵データ	ユーザ情報
⋮	⋮	⋮

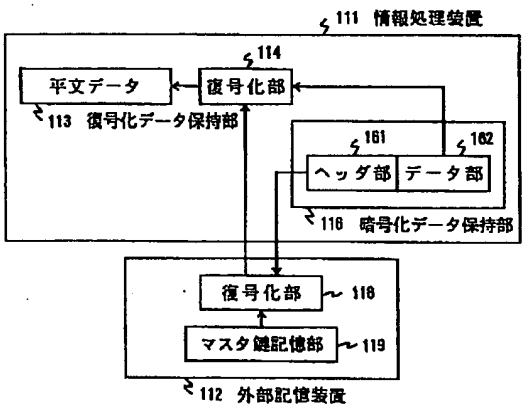
【図１０】



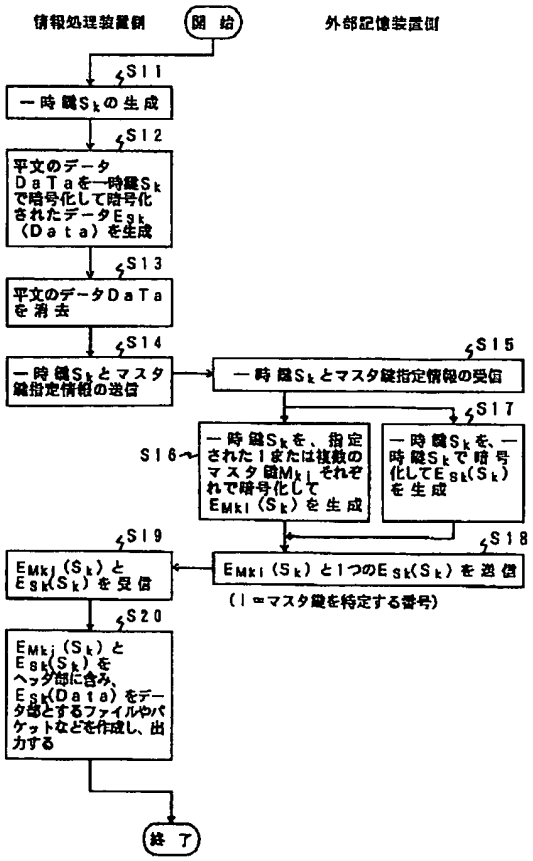
【図１２】



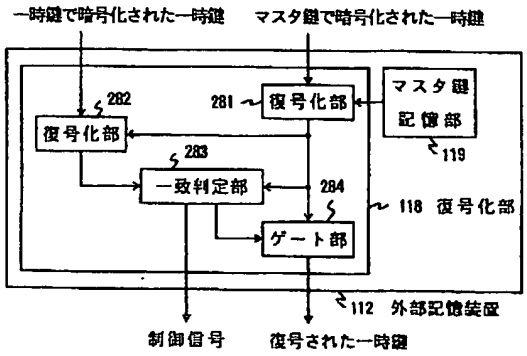
【図１４】



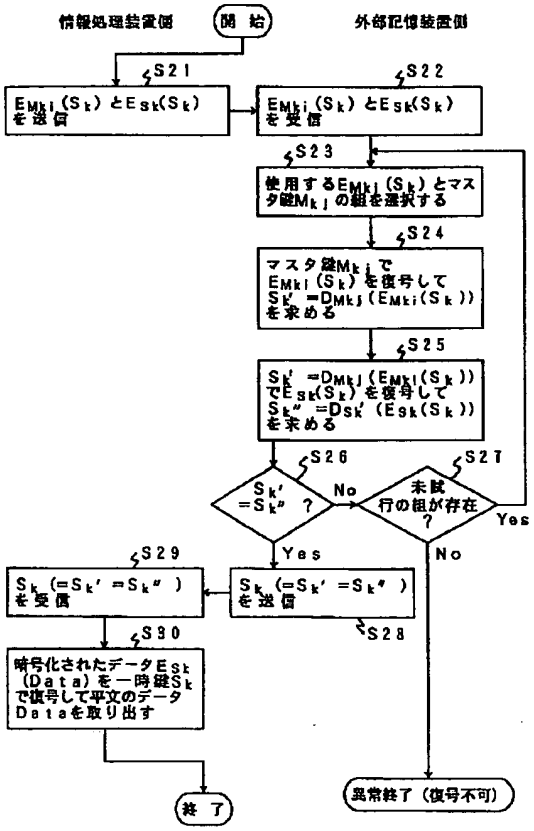
【図１３】



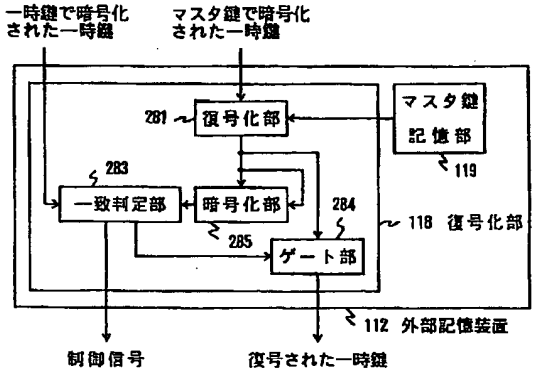
【図１５】



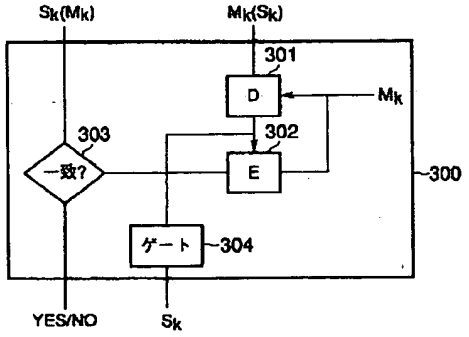
【図１６】



【図１７】



【図２０】

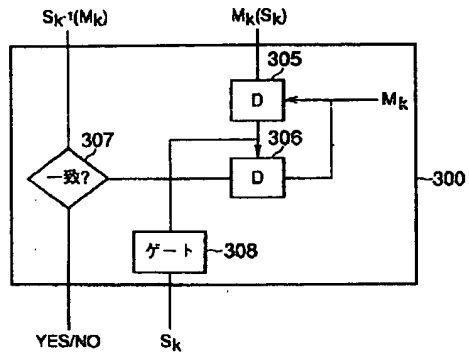


【図１９】

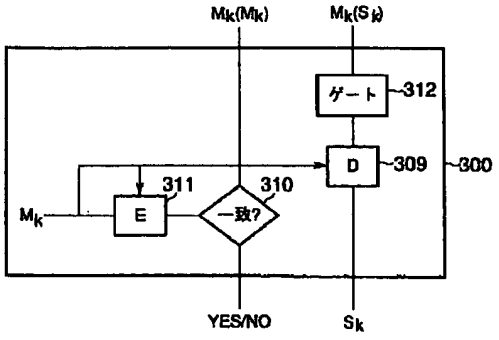
鍵チェック方式 チェック関数

	Mkの暗号化/復号		Skの暗号化/復号	
	含む	含まない	含む	含まない
MkとSk	Sk(Mk) Sk⁻¹(Mk)	h(Mk‖Sk)	Mk⁻¹(Sk) Mk⁻¹(Sk)	h(Mk‖Sk)
Mkのみ/Mkと他のデータ	Mk(Mk) Mk⁻¹(Mk) Mk(Mk+d') Mk⁻¹(Mk+d')	Mk(d') Mk⁻¹(d') h(Mk)		
Skのみ/Skと他のデータ			Sk(Sk) Sk⁻¹(Sk)	Sk(d) Sk⁻¹(d) h(Sk)

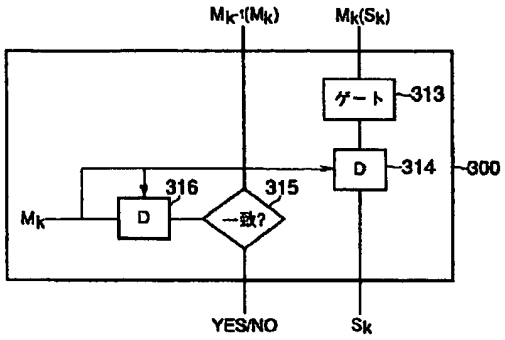
【図２１】



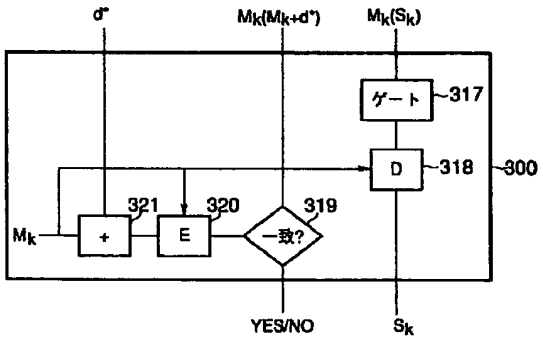
【図２２】



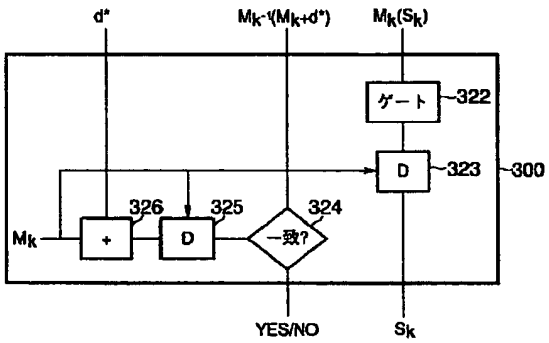
【図２３】



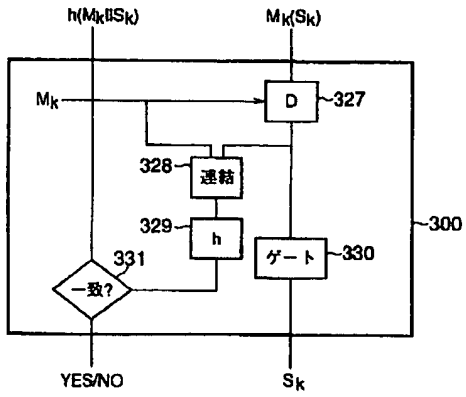
【図２４】



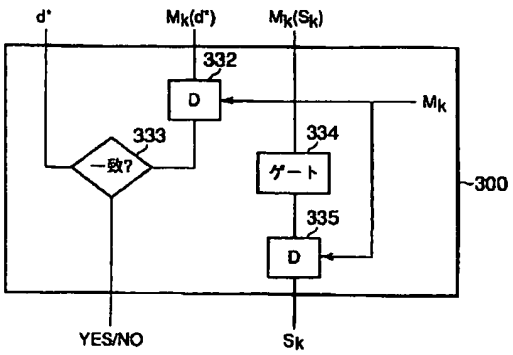
【図２５】



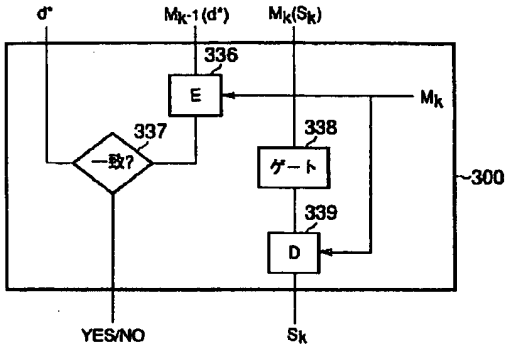
【図２６】



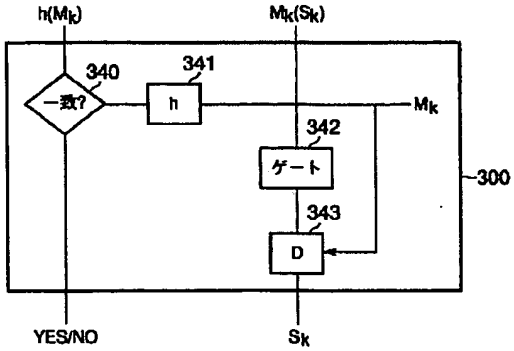
【図２７】



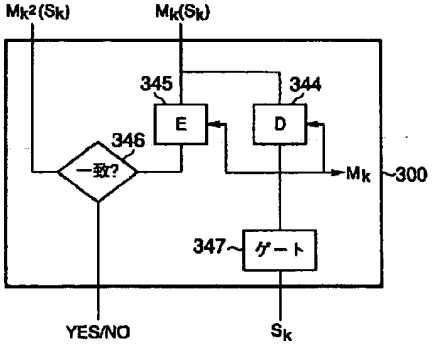
【図２８】



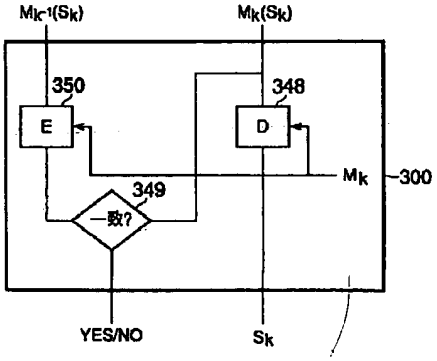
【図２９】



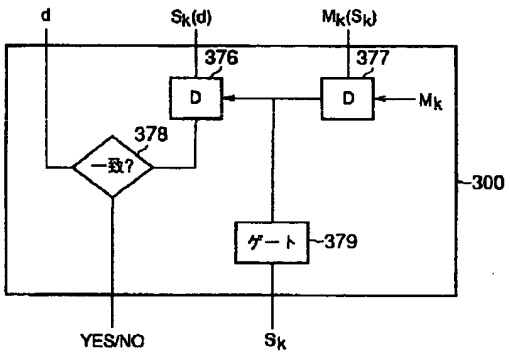
【図３０】



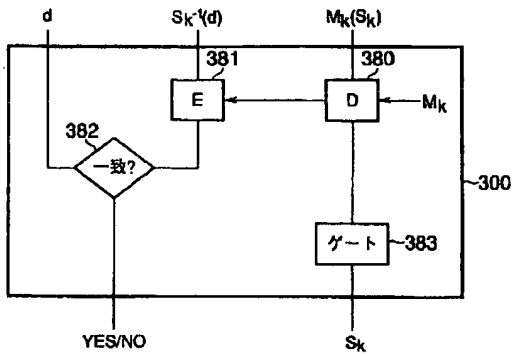
【図３１】



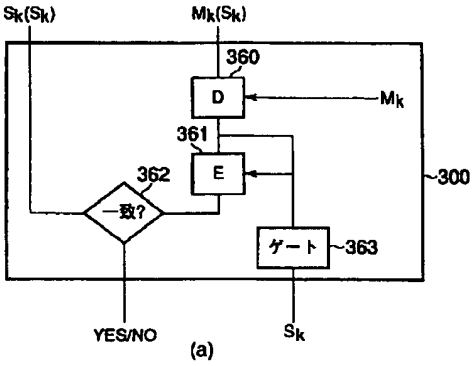
【図３４】



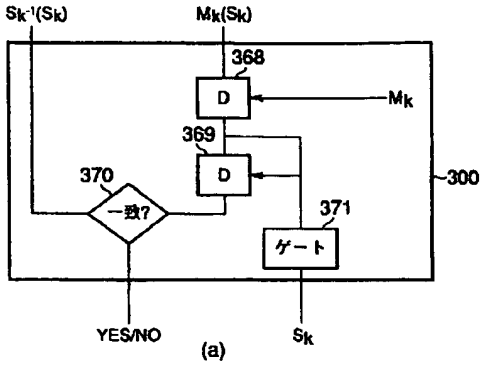
【図３５】



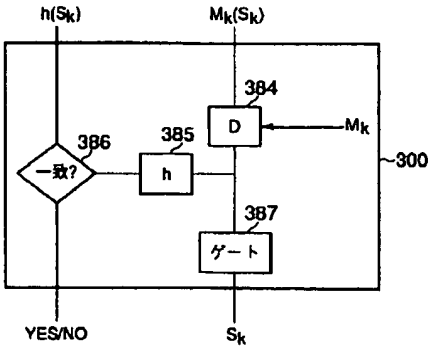
【図３２】



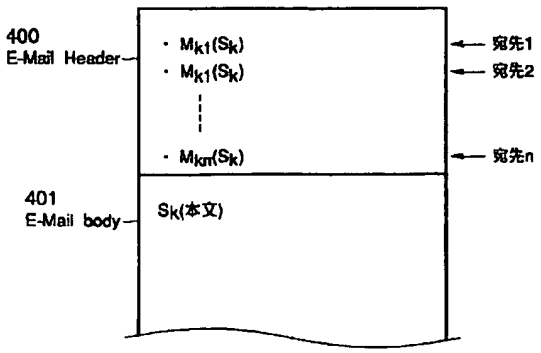
【図３３】



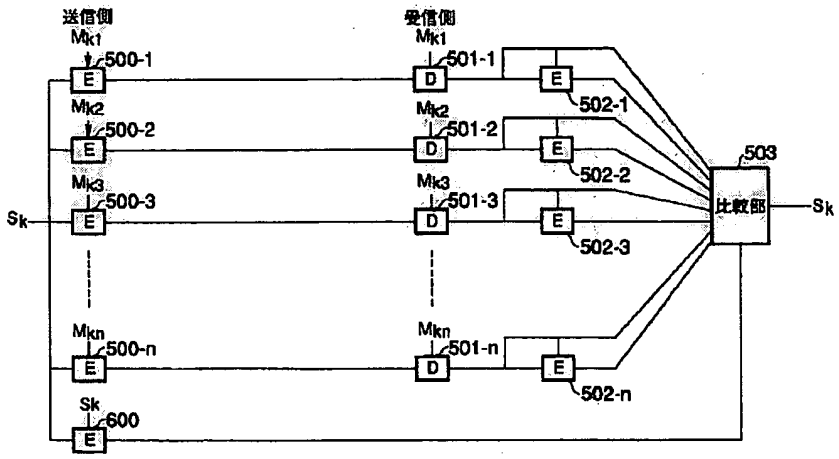
【図３６】



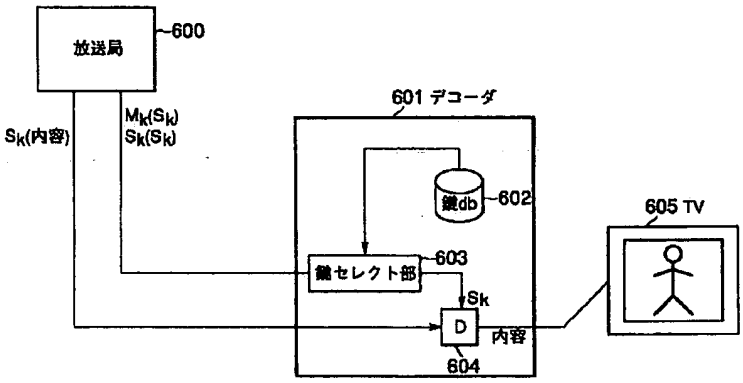
【図３７】



【図３８】



【図３９】



フロントページの続き

(51) Int.Cl.[6]	識別記号	F I	
H０４L　9/10		H０４L　9/00	６２１Ａ

(72)発明者　堀　智美
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内